UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

IN RE: CAPITAL ONE CUSTOMER DATA SECURITY BREACH LITIGATION	MDL No. 1:19-md-2915 (AJT/JFA)
This Document Related to ONLY the following case: MARCUS MINSKY, Individually and On Behalf of All Others Similarly Situated, Plaintiff, vs. CAPITAL ONE FINANCIAL CORPORATION, RICHARD FAIRBANK, ROBERT ALEXANDER, and MICHAEL JOHNSON, Defendants.	Case No. 1:19-cv-1472 (AJT)

AMENDED CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS

TABLE OF CONTENTS

Lead Plaintiff Edward Shamoon, individually and on behalf of all other persons similarly situated, by his undersigned attorneys, for his complaint against Capital One Financial Corp. ("Capital One") and the Individual Defendants (defined below), alleges the following based upon personal knowledge as to himself and his own acts, and information and belief as to all other matters. Plaintiff believes substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

I. NATURE OF THE ACTION

1. This is a securities class action brought on behalf of all persons who purchased or acquired Capital One common stock between July 23, 2015, and July 29, 2019 ("Class Period"), did not sell such shares prior to July 29, 2019, and were damaged thereby. Excluded from the Class are Defendants, all present and former officers and directors of Capital One and any subsidiary thereof, members of such excluded persons' families and their legal representatives, heirs, successors or assigns and any entity which such excluded persons controlled or in which they have or had a controlling interest.

2. Capital One marketed itself to investors as having taken enormous efforts to be the technologically savviest bank, with the best infrastructure, the best software engineers – and the best cybersecurity practices. Capital One lied. In fact, to bolster its technological transformation, Capital One *sacrificed* cybersecurity. It created vast stores of data, called data lakes, containing decades of effectively unencrypted customer data, linked to customer financial information, to which it granted access with reckless disregard for the security of the information. It did not meaningfully encrypt the data contained in the data lakes. When the market learned that an individual hacker had stolen data from 106 million credit card applicants dating as far back as 2005, the market was shocked, and Capital One's stock price fell materially, damaging investors.

3. From its entry into the banking industry in the 1990s, Capital One claimed it would outcompete its more established peers by gathering better information and deriving better models to make better credit and marketing decisions.

4. Defendants have heralded this century's substantial increases in computing power and massive increases in the amount and usability of data. This unfolding digital revolution seemed tailor-made for Capital One's claimed competitive advantage.

5. In 2011, Capital One that it was beginning a digital transformation which would lead to enormous benefits. Defendants stated that the transformation was "revolutionary" and an "amazing opportunity." The Company bragged that "it is just hard to exaggerate how much time and energy" Capital One and its senior executives spent pursuing it.

6. In 2015 Capital One reinforced its commitment to the digital transformation when it announced that it would move all its data from its own private cloud to the public cloud.[1]

7. During the Class Period, Defendants emphasized to investors again and again that Capital One's digital transformation was its single greatest competitive advantage. Defendants claimed that the transformation was "revolutionary" – in fact, that it embodied "the biggest revolution in the history of mankind." Defendants claimed that Capital One benefitted from the "revolution." They claimed that Capital One would be better able to identify profitable customers, send them individualized real-time advertisements and reward offers customized to win their business, and make more informed credit decisions. Defendants claimed that these benefits also

[1] A private cloud consists of computing resources dedicated exclusively to the customer. Capital One had historically placed its data on company-owned servers. Public clouds are computing resources maintained by a third party, not dedicated to any particular customer, in which any given customer simply leases space. The most prominent public cloud, which Capital One and millions of other customers employed, is Amazon Web Services.

allowed them to reach multibillion-dollar partnerships with large retail chains who Defendants claimed wanted to benefit from Capital One's digital resources and know-how. For five years, in numerous statements to investors, Defendants told investors that they should invest in Capital One because it was the most technologically savvy of ***all*** banks.

8. Keeping and storing vast amounts of data raises cybersecurity concerns. Defendants, however, claimed that better cybersecurity was integral to Capital One's digital transformation. According to Defendants, the digital transformation was a "shared path" that would improve Capital One's capabilities, including cybersecurity. Defendants claimed cybersecurity was "incredibly important," "critical," and Capital One's "most important" priority. They claimed that Capital One encrypted all data it stored in the cloud and that it adhered to principles requiring it to respect customers' reasonable views of how long it would hold onto their data. They emphasized that Capital One's reputation for strict cybersecurity would prove a competitive advantage as against purely tech companies. Thus, Capital One would harness its technological savvy to protect its customers' data.

9. According to Defendants, one of Capital One's main weapons in its cybersecurity arsenal was Cloud Custodian, a program Capital One developed in house that Defendants claimed automatically encrypted all the data Capital One made accessible to employees. Thus, even if a hacker penetrated Capital One's firewall, the hacker would still not obtain meaningful data.

10. Moreover, Defendants claimed Capital One complied with principles requiring them to delete customer data after a reasonable time. ***Even if*** a hacker breached Capital One's firewall and ***even if*** the hacker somehow decrypted the data, Capital One's deletion practices would sharply limit the number of customers affected.

11. On July 29, 2019, Capital One announced that a hacker had stolen personal information drawn from 106 million credit card applications ("Data Breach"). The information included, for each applicant, self-reported income, complete demographic information, and last four numbers of social security numbers. The data the hacker obtained also set out information on the customers' subsequent performance (e.g., credit lines, credit scores, payment history, and the like), which would identify for criminals exactly the most profitable identities to steal. The hack also exposed more than 100,000 full social security numbers, and about one million of the Canadian equivalent of social security numbers.

12. The admissions in Capital One's announcement, subsequent reporting, and reports from former employees show that Capital One had sacrificed cybersecurity to a dangerous extent, belying their repeated claims to the contrary. Given Capital One's deficient cybersecurity measures, the Data Breach was inevitable.

13. The foundation of Capital One's digital transformation was machine learning, a process through which computer algorithms are given raw data and "learn" on their own to discern patterns and accomplish tasks. More data means better algorithms.

14. To optimize machine learning, Capital One created massive data lakes (i.e., repositories of customer data) containing data retained far in excess of customer expectations. Capital One announced that the hacker had stolen data from credit card applications submitted as early as 2005. Capital One had held on to this data for fourteen years. To ensure that the information the algorithms gleaned was as useful as possible, Capital One also included outcomes (the customer's subsequent performance). Capital One made so much data accessible that any breach would be catastrophic.

15. Capital One former employees spoke to the chaos Capital One's access "controls" created. A former employee who headed the unit that developed Capital One's digital cybersecurity infrastructure reports that each Capital One line of business created its own data lakes of customer data. The former cybersecurity infrastructure employee reports that each division could determine who had access to its own data lakes and the terms of that access – leaving Capital One only as secure as its least secure division. A former employee in Capital One's cybersecurity division reports that Capital One kept over 500 million usernames and passwords on its server on an unencrypted plaintext spreadsheet, searchable and accessible to anyone. Indeed, between 2017 and 2019, Capital One reported at least four incidents in which insiders exploited overbroad access and weak monitoring to access multiple Capital One customers' data – ***far*** more than any other bank.

16. Finally, contrary to Defendants' express statements, Capital One's data was not meaningfully encrypted. Rather than limiting decryption to relevant persons, Capital One automatically decrypted data for ***any*** person with Capital One credentials. As an expert explained, Capital One's encryption was "academic at best."

17. Capital One's loose and chaotic access policies, huge numbers of vast data lakes, and automatic decryption made a hack like the Data Breach inevitable. With too many authorized requests by Capital One employees and algorithms to access data to monitor, an illegitimate request would be difficult to catch. Indeed, the hacker involved in the Data Breach accessed Capital One's data three times in March and April 2019 and used Capital One's computer resources to mine bitcoin, without ever being detected.

18. The final weakness in Capital One's cybersecurity defenses was Defendants themselves. In 2017, Capital One hired Michael Johnson to be its Chief Information Security

Officer ("CISO"), the head of the cybersecurity division. Defendants considered turnover in that division material and closely monitored it, including in reports to Capital One's board of directors. Johnson immediately alienated the cybersecurity division's employees. The division's turnover in 2018 was about one third. Under Johnson, Capital One's cybersecurity division even omitted to take elementary precautions like installing security software Capital One had purchased.

19. The July 29, 2019 announcement of the Data Breach thus was the inevitable result of Capital One's abandoning cybersecurity practices to carry further itsd business plan.

20. Defendants' boasts that Capital One would use its vast technological savvy to protect and encrypt customer data deceived investors. On July 30, 2019, the day after Capital One disclosed the data breach, its stock price fell 6% on exceptionally high volume of trades to close at $91.21, damaging investors.

II. JURISDICTION AND VENUE

21. The claims asserted herein arise under Sections 10(b) and 20(a) of the Exchange Act (15 U.S.C. §§78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17 C.F.R. § 240.10b-5).

22. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §1331 and Section 27 of the Exchange Act (15 U.S.C. §78aa).

23. Venue is proper in this Judicial District pursuant to 28 U.S.C. §1391(b) and Section 27 of the Exchange Act (15 U.S.C. §78aa(c)). The Company's headquarters are located in this district.

24. In connection with the acts, transactions, and conduct alleged herein, Defendants directly and indirectly used the means and instrumentalities of interstate commerce, including the United States mail, interstate telephone communications, and the facilities of a national securities exchange.

III. DEFENDANTS AND RELEVANT THIRD PARTIES

25. Court-appointed Lead Plaintiff Edward Shamoon, as set forth in his Certification, which was previously filed on the Court's docket and is incorporated by reference, purchased Capital One common stock during the Class Period at artificially inflated prices during the Class Period and was damaged thereby.

26. Defendant Capital One is a bank holding company. Capital One differentiates itself from competitors by boasting of its focus on technology. Defendant Fairbank summarizes Capital One's purported competitive advantage by claiming that among banks it alone is "an information-based technology company that does banking competing against banks who use information and technology." Capital One's shares trade on the New York Stock Exchange under ticker COF. Capital One has three main lines of business: credit cards, auto loans, and commercial loans. During the Class Period, credit cards accounted for a large majority of Capital One's revenues. Included in this category were substantial revenues from issuing store-branded credit cards to retail chain partners like Walmart.

27. Defendant Richard Fairbank founded Capital One and has served as its CEO at all times.

28. Defendant Robert Alexander joined Capital One in 1998 and has served as its Chief Information Officer ("CIO") since May 2007. According to Capital One's proxy statements, Alexander oversees all of Capital One's technology activities, which included 9,000 employees, more than 8,000 of whom were software engineers.

29. Defendant Michael Johnson served as Capital One's Chief Information Security Officer ("CISO") from March 2017 until he was terminated in October 2017 because of the Data Breach. Johnson met with Capital One's Risk Committee, a committee of its board, at least twice

a year. Johnson headed Capital One's Information Security & Risk Management Division which during Johnson's tenure was renamed the Cybersecurity Division.[2]

30. Fairbank, Alexander, and Johnson are the "Individual Defendants."

31. Former Employee 1 ("FE 1") worked for Capital One between December 2015 and November 2018. During the first year of his tenure, FE 1 was an Information Risk Manager in the Cybersecurity Division reporting directly to the CISO. Thereafter, FE 1 headed the Capital One division responsible for developing and implementing Capital One's cloud security policies and governance.

32. Former Employee 2 ("FE 2") worked for Capital One between October 2016 and July 2017 as a Senior Manager in Capital One's Cybersecurity Division. FE 2 reported to a Director in the Cybersecurity Division who in turn reported to Richard Isenberg, VP of the Cybersecurity Division, who reported to the CISO. FE 2 has senior government experience, including briefing the head of a law enforcement agency.

33. Former Employee 3 ("FE 3") worked for Capital One as a Cyber Security Incident Manager between 2016 through 2018. FE 3 headed a cyber incident team whose functions included observing operations, compiling indicators of compromise, and sending suspicious activity reports. FE 3 reported to a Director in the Cybersecurity Division, who in turn reported to a Senior Director, who reported to Defendant Johnson.

[2] "Cybersecurity Division" as used herein refers to the division both before and after the name change.

IV. BECAUSE THEY FIXATED INVESTORS' ATTENTION ON CAPITAL ONE'S DIGITAL TRANSFORMATIONS, DEFENDANTS' STATEMENTS ABOUT CYBERSECURITY WERE CRITICAL TO INVESTORS

A. From Its Founding, Capital One Distinguishes Itself By Its "Information Based Strategy"

34. Capital One, founded as another bank's credit card division, was spun off in 1994. Capital One has always told investors that it would thrive by using more data more intelligently than its competitors.

35. After the spin-off, the only financial product Capital One offered was credit cards. Its narrow offering differentiated it from other credit cards companies, which tended to be large banks offering many different products. Capital One's narrow offering made it a much riskier bet than its competitors, as its diversified competitors could weather a downturn in the credit card market that might be enough to put Capital One out of business. Capital One focused its business on riskier subprime customers.

36. To lower its risk, Capital One followed a strategy it had adopted in 1988 which it called its *Information Based Strategy*.

37. Capital One's 1996 10-K, its very first, explained:

> The Company's IBS [i.e., Information Based Strategy] is designed to allow the Company to differentiate among customers based on credit risk, usage and other characteristics and to match customer characteristics with appropriate product offerings. IBS involves developing sophisticated models, information systems, well-trained personnel and a flexible culture to create credit card or other products and services that address the demands of changing consumer and competitive markets. By using sophisticated statistical modeling techniques, the Company is able to segment its potential customer lists based upon the integrated use of credit scores, demographics, customer behavioral characteristics and other criteria. By actively testing a wide variety of product and service features, marketing channels and other aspects of its offerings, the Company can design and target customized solicitations at various customer segments, thereby enhancing customer response levels and maximizing returns on investment within given underwriting parameters. Continued integrated testing and model development builds on information gained from earlier phases and is

> intended to improve the quality, performance and profitability of the Company's solicitation and account management initiatives. The Company applies IBS to all areas of its business, including solicitations, account management, credit line management, pricing strategies, usage stimulation, collections, recoveries and account and balance retention.

38. Thus, Capital One maintained ***since its inception*** that its Information Based Strategy would allow it to better identify better customers, better market to them, and offer them rewards better targeted to their wants and needs. By having better information and models than its competitors, Capital One bet that it could also extend credit more intelligently than its competitors, and therefore more profitably, than its competitors.

39. After the spinoff, Capital One began to offer what it called Second Generation Products in markets where it believed it could use its Information Based Strategy to outcompete other banks. These products also targeted moderate income customers or those with poor credit ratings. Capital One maintained that it could turn a profit by using its Information Based Strategy to better evaluate, price, and monitor credit risks.

40. As information technology improved throughout the 1990's and 2000's, Capital One's Information Based Strategy became digital. For example, Capital One's 2000's 10-Ks stated that it "leverage[s] information technology to achieve our business objectives and to develop and deliver products and services that satisfy our customers' needs [a key aspect of which is] the development of efficient, flexible computer and operational systems to support complex marketing and account management strategies and the development of new and diversified products."

41. According to Defendants, Capital One's competitive advantage in information and analysis becomes more material with each passing year. On a call to announce Capital One's Q4 2014 earnings, on January 22, 2015, Defendant Fairbank explained that the technological transformation was critical because it would affect "even something that's very, very core to how

Capital One works, which is information-based strategies itself." Indeed, in that same call, Fairbank called Capital One a "fanatical information-based company; and across all the segments and sub-segments we're in, we are reading the data that is coming back and readjusting constantly our choices and so on."

B. Capital One Went "All In" On A "Revolutionary" "Amazing Opportunity": A Digital Transformation

42. In 2011, Capital One promoted the start of a complete overhaul of its operations, which it called a digital transformation. Deriding banks that merely added apps or online banking to their traditional structures Capital One claimed the main promise of the digital transformation was the ability to use new machine learning technology to boost Capital One's Information Based Strategy. Capital One could create a better experience for customers through (among other things) better credit decisions, better marketing, and better fraud detection systems. To do so, Capital One would have to modernize its entire infrastructure.

43. In 2015, as part of its digital transformation, Capital One announced that it would move substantially all of its computing operations and data to the cloud. In 2016, Capital One announced that it would make Amazon Web Services ("AWS") its predominant cloud provider.

44. As SVP Global Finance Norris explained at the J.P. Morgan FinTech & Specialty Finance Forum on November 30, 2016:

> AWS [Amazon Web Services] announced yesterday after the close an agreement with Capital One where we're making AWS our predominant cloud partner, and we're really migrating a lot of things to the cloud: big data infrastructure and capabilities, cloud computing, the kind of modern infrastructure that's needed to support a truly digital enterprise.

45. Defendants represented, over and over and over again, that its digital transformation was Capital One's single greatest competitive advantage. Capital One boasted that it had the most and the best software engineers and other technology professionals. Capital One executives

acknowledged that they understood investors were hanging on every word they spoke of their digital transformation.

46. Defendants maintained that Capital One's digital transformation was already creating substantial benefits, including multibillion-dollar partnerships with large retail chains excited about Capital One's technology.

(a) The Digital Transformation Was An Opportunity For Capital One To Employ Its Purported Technological Savvy To Outpace Its Competitors

47. In a maxim Defendant Fairbanks frequently repeated, including at the June 1, 2017 Sanford C. Bernstein & Co. Strategic Decision Conference, Capital One was "an information-based technology company that does banking competing against banks who use information and technology."

48. Armed with this advantage, Capital One would leave behind its competitors, who Capital One claimed merely bolted technology onto traditional banks.

49. Before and during the Class Period, Defendants characterized Capital One's digital transformation as the single most important fact about it. In a November 30, 2016 presentation before the J.P. Morgan FinTech & Specialty Finance Forum, Capital One SVP of Global Finance Jeff Norris boasted that "I've been with Capital One for almost 20 years, and this is a rare kind of time in my experience at Capital One in that this investment in digital and digital transformation in banking is one of the few things I think we've ever seen that's just sort of, over time, good on every dimension." Norris added that the digital transformation is "an integral part of our card growth, and over time I think it just becomes more and more the company we are [] and we believe is one of the cornerstones of our strategy."

50. Defendant Fairbank was even more enthusiastic.

51. On a call to announce Capital One's Q4 2014 earnings, taking place on January 22, 2015, Defendant Fairbank said that:

> And finally, the investment in digital. And while digital is a big opportunity across consumer and commercial, certainly, on a relative basis, I think the revolution is going to be greater on the consumer side and it's literally going to transform all aspects of how banking is done. It's going to transform not only – people often think through the lens of the customer experience, but really the whole way, the way retail distribution works, the way operations, marketing, servicing and even something that's very, very core to how Capital One works, which is information-based strategies itself. So this is a big deal on the commercial side***. It's pretty much a revolutionary deal on the consumer side***.

52. Fairbank added that "I haven't seen anything remotely like this in terms of the ability to transform how a business works."

53. At the February 10, 2016 Credit Suisse Financial Services Forum, Fairbank reiterated that "[t]his is the most significant thing I've seen in the 25 years of building this Company in terms of opportunity but also in terms of like risk if you don't really go for it."

54. At the June 2, 2016 Sanford C. Bernstein & Co. investor conference, Fairbank claimed that:

> The most important place, the most important things that are going on are not the things that you can readily see***. It's about foundational technology that is the shared path to really being a digital company.*** It's about the information-based strategy that we use in credit decision-making, in marketing, to be able to originate and book the accounts of the quality that we have.

55. On an April 25, 2017 call to discuss Capital One's Q1 2017 earnings, Fairbank pointed to the "significant investment Capital One has been doing in transforming our company in response to the biggest revolution in the history of mankind [i.e., digital] and something that's going to absolutely transform banking and is only in the very early stages of doing that."

56. Indeed, On a January 24, 2017 conference call to announce Capital One's Q4 2016 earnings, Fairbank noted that he had talked about the digital transformation "many, many times" "for a long time":

> Important places we're investing is, as we talked many, many times, is on the digital side and, as I've said for a long time, the digital transformation of us really into – to operating like a technology company that's not a one or two or three years' thing. That is a transformation that in many ways is a lifetime transformation.

57. Capital One executives were focusing their attention on the digital transformation. As Fairbank announced at the Barclays Global Financial Services Conference taking place on September 11, 2017, that ***"[I]t is just hard to exaggerate how much time and energy we -- myself personally, but we, our company, our team, our senior team, put into the digital revolution trying to understand it, understand where it's going and then understand what does it mean for us***."

58. On an October 23, 2018 call discussing Capital One's Q3 2018 earnings, Defendant Fairbank noted that the digital transformation "is the most important thing, it's the thing every company needs to be spending more time talking about." He added that "it is very clear that banking is going to be totally transformed and everything about how a bank works as it is experienced from the outside and how it works on the inside are going to need to change in order to, in the end, deliver real-time, intelligent, digital customer experiences."

59. Defendants understood the need to speak carefully about the digital transformation given that they emphasized its materiality to investors. In a November 6, 2015 presentation at the BancAnalysts Association of Boston Conference, Capital One CFO Stephen S. Crawford ***refused to answer*** a question seeking information about the digital transformation because "given the focus that our investor base has on the words [regarding digital transformation], we spend a lot of time thinking about exactly what it is we want to say."

60. Likewise, Defendants had a policy of not providing guidance, but made an exception when it came to metrics affected by the digital transformation. As Fairbank explained on a June 23, 2015 call to discuss Capital One's Q2 2015 earnings, "[s]o the reason that we took the time here to la out [metric] guidance [] was just to give you a sense of the commitment that we

have to investing on the digital side and the commitment that we have to seizing the opportunity on the card growth side." Defendants would continue to provide guidance on that same metric through the end of the Class Period.

61. Defendants claimed that the digital transformation was succeeding because Capital One was able to attract the best tech talent in America.

62. To attract tech talent, Capital One had to position itself as a forward-leaning company. As Defendant Fairbank explained at the Sanford C. Bernstein & Co. Strategic Decisions Conference on June 2, 2016, to avoid seeming like a "stodgy bank" to tech employees, Capital One had to let engineers bring their ideas to market quickly:

> [Y]ou've got to attract the very best tech talent, and this is the talent that is the most sought-after jobs in America. Winning in technology absolutely means winning in recruiting. Recruiting isn't about speeches you give or what you pay. Recruiting is about what they find when they come, which immediately the first thing they look at is what technology do you have, what am I going to work on? And then, right – the next thing is how does the company work, what's the nature of the work environment? Can we get stuff done? ***Does this feel like a stodgy bank or does this feel like a tech company? And finally, they look at what product is being shipped at the other end of this thing. And there is a virtuous circle that comes from attracting better talent, investing in great technology, having a dynamic, fast-paced place to work and shipping great product*** [.]

63. Fairbank added that:

> I think what I'm most excited about our own technology journey is not necessarily manifested in some of those external things you see. But in many ways, the best place to look is look at the technology recruiting marketplace. Where is tech talent going? How much of it is going into the – great tech talent, how much are they considering financial services companies? When they think of banks, they probably think boring, old-school kind of things. How much traction is a company getting in that marketplace? ***I think Capital One is getting a lot of traction in people realizing, wow, this is a lot more like a tech company than I thought and, in many ways, a lot more than a tech company than a bank.***

64. Defendant Fairbank further explained at the Goldman Sachs U.S. Financial Services Conference taking place on December 6, 2017 that unlike "boring banks", Capital One let its engineers "ship product":

> The key thing there, and whether those things are successful, is very much is what is – does the company that's being bought, particularly if you want to keep the talent, ***do they feel they're being bought by a tech company or some boring bank?*** And as we have continued to transform the company, and as I often say, build an information-based technology, a company that happens to do banking, that's a very different model than a bank that happens to use information and technology. And one of the most striking places you see that is in the recruiting marketplace and the increasing brand that Capital One has, both in recruiting and even on the small acquisition side to be a company ***where tech people can really feel at home and they feel they can come in and they can, in their language, ship product instead of coming in and banging their heads in a world of traditional technology.***

65. Crawford added at the November 4, 2016 BancAnalysts Association of Boston Conference, that with respect to digital, "if you're not forward-leaning with respect to the tools, the way that you approach problems, you're going to not be successful with your employee base."

66. Indeed, speed was of the essence at Capital One. As Fairbank explained on a July 20, 2017 call to discuss Q2 2017 earnings:

> I also said that the biggest motivator of our digital investment is not a cost objective. It really is a much better customer experience. ***Building a way more dynamic, well-managed, fast, first-to-market, better controlled***, all those other kinds of benefits that come with this.

67. Capital One CFO Stephen S. Crawford added at the November 4, 2016 BancAnalysts Association of Boston Conference, that "[s]o we're bringing in technologists that are program designers, who are data analysts, who are experts in machine learning and big data."

68. Capital One increased the number of software engineers it employed from 2,500 in 2011 to 9,000 in 2019.

69. Defendants were clear and repetitive – the digital transformation was Capital One's future and the single most important reason investors should buy Capital One's shares.

70. At the June 11, 2017 Sanford C. Bernstein & Co. investor conference, Fairbank noted that Capital One must "go all in with digital." He closed his presentation by pleading with investors to focus on Capital One's technological capabilities when they made investment decisions:

> The opportunity to build an information-based technology company that does banking, competing against banks that are more traditional in what they do and competing against tech companies that have a lot of advantages, but there's a number of things that hold them back – ***There's an amazing opportunity in this transforming world of banking. [] This feels more like the founding days than it has at any time in the last 20 years. So that's the movie trailer relative to future things.***

(b) Defendants Tout the Promise of the Digital Transformation's Incorporation of Machine Learning to Dramatically Intensify Capital One's Information Based Strategy

71. Defendants told investors that lower costs through software and better digital apps were only a small part of the benefits investors should expect from Capital One's digital transformation. The real benefit would come from using machine learning to improve customer experience.

72. On a conference call to announce Capital One's Q1 2018 earnings taking place on April 24, 2018, Defendant Fairbank acknowledged that "there are many benefits that come from" investing heavily in technology "and cost to me isn't even at the top of the list and we're not doing it primarily for cost benefits." At the February 10, 2016 Credit Suisse Financial Services Forum, Fairbank stated that "cost is probably only fourth or fifth on the list of the benefits that come from digital." And as Jeff Norris acknowledged on the November 30, 2016 J.P. Morgan FinTech & Specialty Finance Forum, "think of that 10% of the technology iceberg as sort of customer-facing apps, and then it'll make more sense when I say that the vast majority of the investment agenda we have for digital transformation is that 90% that's below the surface." Rather, Capital One executives consistently referred to the "foundational stuff" as the use of machine learning employed on vast sets of customer data to pursue Information-Based Strategies at a far superior level of sophistication.

73. For example, as SVP Global Finance Norris explained at the J.P. Morgan FinTech & Specialty Finance Forum on November 30, 2016, "[c]ost is an important thing, efficiency is an important thing, ***but in some ways it's almost the least important thing.***"

74. And as Defendant Fairbank explained on a January 22, 2015 call to report Q4 2015 earnings, in connection with Capital One's digital investments, "what I'm most interested about [in connection with the digital transformation] is actually the opportunities to generate growth and to generate better real-time decision-making, to make better credit decisions, and in the end to build a deeper franchise through very significant improvements in the customer experience and things that really create more loyalty and more stickiness with customers."

75. Fairbank insisted on a call to discuss Capital One's Q1 2015 earnings, taking place on April 23, 2015, that the digital transformation:

> In some ways, I mean it's a lifelong, forever journey. This is not like we're going to say next year, we're going to be real-time. I'm just saying, so from a journey for me that started 20 years ago and looking at the banking industry and saying in many ways this is really the information business, not necessarily just the traditional banking business***. I'm saying the world – it's very clear at the accelerating rate that the world is moving, the ability to – the dimensions of how information is leveraged, the real-time nature of information and the software revolution that has changed everything, the connected revolution here.***

76. Fairbank returned to the theme of using big data to pitch customized products to consumers at the Sandford C. Bernstein Strategic Decisions Conference taking place on May 28, 2015:

> ***And if I were to describe [the benefits of digital] it is way faster product development, way better products that are integrated into people's lives, way better insights from data and, ultimately, the ability to create customized solutions in real time that right now we all live on a batch basis.***

77. Moving to the cloud was essential for Capital One's digital transformation. As Capital One CFO R. Scott Blackley explained at the Morgan Stanley Financial Services Conference on June 14, 2017, "[w]e think we can differentiate ourselves [because of the digital

transformation] by virtue of our ability to have [] great access to data and our ability to harness that data to do different things." Blackley continued:

> The idea that you run a bank on a batch cycle, where you have processing that happens at the end of every day, and you aggregate that up, it makes us slow and it's hard to – I don't think that the – market of the future is really more about how you can do things quicker and more real time as opposed to having to wait. So a lot of the digital work we're doing is to set us up to be a more real-time company.
>
> * * * * *
>
> ***I think the next wave is where you really start to see some amazing things, where things like machine learning, robotic automation, all those things really – you've got to have this data foundation and this technology foundation we've been putting into place over the last several years.***

(c) Defendants Boast That Capital One's Digital Transformation Was Providing Substantial Immediate Benefits

78. Capital One used machine learning data analysis to pursue two main business advantages: squeezing more profits out of credit card customers and securing partnerships with large retail chains.

79. As Fairbank explained at the June 1, 2017 Sanford C. Bernstein & Co. Strategic Decision Conference, Capital One would use big data to identify and retain "heavy spenders," affluent customers who spent heavily on their credit cards, always make on time payments, sometimes roll over their balances but always pay them off:[3]

> [W]e have a huge investment and a lot of very successful techniques for customized marketing and a lot of it on the digital space. Speaking of digital***, I think the next frontier where there will be differentiation in the heavy spender business will be on digital capabilities.*** Capital One is putting a huge investment into technology, a huge investment in unique and differentiated digital product offerings. This is an area that we look to certainly differentiate ourselves over time.

[3] As Defendant Fairbank explained on an April 25, 2019 call to discuss Capital One's Q1 2019 earnings, "Heavy spenders are hard to get but exceptionally valuable to have. They are long-term annuities that pay off on the bottom line with strong interchange revenue, loan balances from occasional revolving, very low charge-offs and very low attrition."

80. Capital One also sought out partnerships with large retailers, chiefly in the form of branded cards in which both partners would share the benefits and costs. There, too, Capital One touted technology as its competitive advantage. As Defendant Fairbank explained on a call to discuss Q1 2015 earnings taking place on April 23, 2015:

> As you know, the retailing business, for example, is in massive strategic turmoil. ***And the impact of digital and the need for retailers to reinvent themselves is an extraordinary in many ways kind of existential kind of imperative. And I think that companies like Capital One that are doing very significant investments in digital and in mobile and in not just the customer experience that is associated with that but all the underlying infrastructure that is behind what it takes to actually innovate in digital, companies like ours.*** I think are in a very good position to partner with retailers and help them strategically and actually in terms of real product innovation and execution in that transformation. So we are also investing in that opportunity and we have partners with whom we're working right now on some pretty cool digital innovations.

81. Jeff Norris, SVP Global Finance, expanded on these claims at the Barclays America Select Conference on May 20, 2015:

> If you're a physical retailer, you're not really sure why a customer came into your store, right. Is it because you had a really successful advertisement in the Sunday newspaper? Or is it because it was a nice day and they decided to go out and go shopping? It's a one-off transaction, and you don't really capture a lot of information or relationship benefits from those one-off sales transactions.
> ***A card partnership is an opportunity for retailers to develop more of an ongoing dialogue and an ongoing relationship with their retail customers. And we feel like there's a lot of customer relationship benefits that we can help retailers unlock using our information base in more analytical approaches. So we really want to be in partnership with retailers that view the card opportunity that way as opposed to merely an opportunity to monetize customer relationships.***

82. Indeed, because of its existing investments in digital technology, and because it could work with multiple retailers at the same time, Fairbank explained at the Sandford C. Bernstein Strategic Decisions Conference on May 28, 2015 that Capital One would benefit from substantial economies of scale:

> As just one example on that [] this is also a business where we can add a lot of value to a retailer. The elephant in the living room of retailers is the digital revolution. ***And there is a great opportunity for banks like ourselves that are investing very significantly in digital***

innovation to help retailers in their own journey and some scale – economics of doing that for multiple retailers.

83. Fairbank further boasted on the same call that Capital One's digital capabilities would be transformational for retailers:

> So, it's always been a natural inherent advantage in some ways for the players who have skew level data, and I think if I were at those companies, we're doing everything we could to take advantage of that, and I think there is value for retailers. There is the whole area of information-based strategies, their analytical opportunities for retailers are everywhere. But just looking at their customer base, looking at loyalty programs, watching what drives same-store sales growth, what works from a marketing point of view, how to create really good test and control, how different rewards, choices make a big difference on the credit side, the whole role of selection and positive selection and negative selection. The incredible difference that exists for a retailer between those who are motivated on a private label program to – for the making of money as opposed to players like Kohl's who are motivated for the building of – using a private label program as the central nervous system of building a franchise. The extraordinary difference is that happen when you're all in on the latter as opposed to the former and helping customers along the way. And then, of course, you have the digital revolution and not only the opportunity to help create digital product, but also to get to the – even greater opportunity, which is the fusion of digital capabilities and measurement that comes along with that. And retailers are at a very, very early stage of that, frankly banks in general, banks like Capital One has spent a lot more years investing in that very thing. ***So our value proposition for private label companies is to help them take advantage of some of the scale investments that we make in these areas of digital and information-based technology, and share the technology and the know-how with them.***

84. Fairbank returned to the same point three years later, on July 19, 2018, during a call discussing Capital One's Q2 2018 earnings:

> Well, so there's kind of two approaches to a partnership business. One can build a lot of custom technology associated with any particular partner, or on the other hand, one can build general capabilities that would be very compatible with partners who are really looking to build a franchise. And the way our tech transformation has happened by design, which is really about building foundational technology and sort of working up the technology stack to create a lot of digital capabilities and flexibility within our Card business, that is a very natural thing to bring into the partnership business.
> ***So our philosophy is more create a way that we can help our partners ride on our technology path, as opposed to go create a new technology path one partner at a time. [] So as we've said over the years that one of the benefits of our tech investment should be our ability to be a better partner out there.***

85. Defendants continued to highlight that Capital One's digital transformation would prove attractive to investors. As Defendant Fairbank explained in a call to discuss Capital One's Q2 2018 earnings taking place on July 19, 2018:

> If you look at the spectrum of card partnerships out there and essentially the partners behind those card partnerships, on the one end of the continuum are ***the partners who view the card program as [an] essential element for building a franchise and deepening customer relationships.*** The other end of the continuum is partners who sort of view the card program as a profit center.
> ***And we have consistently kind of tried to focus on the former end of the spectrum, because not only is that where we think the better opportunity lies, also the value that we have to add, what we can bring to the table in the context of our digital capabilities and underwriting and marketing, would be consistent with those players who really are looking to card partnerships as a means to grow and really build a franchise.***
> And however important card partnerships were in the past, I think we should all understand they're more important in the emerging digital world, just because of the centrality of how payments play in the digital e-commerce environment relative to – in the physical environment.

86. On July 26, 2018, Capital One announced that it had reached a long-term agreement to become the exclusive issuer of Walmart's cobrand and private label credit card program in the U.S. Capital One also agreed to acquire Walmart's existing portfolio, which Capital One expected would consist of approximately $9 billion of receivables. On a call to discuss Q1 2019 earnings taking place on April 25, 2019, Defendant Fairbank claimed that "I think our tech transformation was central to winning the Walmart deal."

(d) Defendants Told Investors That the Digital Technology Would Improve Customers' Perceptions of Capital One

87. Defendants told investors that the Digital Transformation would be a competitive advantage for Capital One because it would make Capital One more appealing to customers.

88. On a July 20, 2017 call to discuss Capital One's Q2 2017 earnings, Fairbank told investors that the single best benefit of the digital transformation is its power to "delight[]" customers:

> So, where can you see the benefits [of Capital One's digital transformation]? No one can disentangle what – ***no one can prove what happens when your customers are a lot more delighted***, how that affects things like growth and retention and things like that, but I just would say that – and it's very easy, Brian, for you to – I'm not going to rattle them all off here – there's a lot of various proof points associated with a dramatic increase in Capital One's – the customer satisfaction, go to the App Store and look at their ratings on the App Store, between the digital experience, the customer experience, go to our own website and look at the ratings that – and reviews that people put up on our own account.
>
> For a variety of reasons, one of which is our digital transformation, we have had a tremendous momentum with customers that is pretty linked to the kind of exceptional growth that we have seen. Look in the auto business, I don't know if you've seen some of the technology that we're employing in the auto business associated with Auto Navigator. I would suggest you take a look at that, that's pretty interesting. ***I can never prove you to what the contributions of delighted customers are on the growth front.***
>
> Secondly, on the marketing front, there is an obvious and dramatic transformation going on in marketing and how it works and the growing role of digital marketing. Digital marketing itself has got the word digital in it. And it's about digital capabilities. And in fact, information-based strategy, that has been an important contributor to Capital One's success.
>
> * * * * *
>
> ***I also said that the biggest motivator of our digital investment is not a cost objective. It really is a much better customer experience. Building a way more dynamic, well-managed, fast, first to market, better controlled, all those other kind of benefits that come with this.*** All of that said, it's very clear that we are increasingly reaping important sizable benefits and efficiency as a result of years of digital investment, and the efficiency comes across distribution channels of retail, call centers, operations, centers. The transformation in how we work as long-term benefits, many of which we've started to realize. So the interesting thing is a journey that was never motivated to be, number one, for the sake of cost savings. Something where it cost a lot, the costs were a lot higher than the benefits at the outset, those relative meters are on their way to some significant change in position there. And so it is the efficiency ratio would be the final place that I would point to.

89. Fairbank's July 20, 2017 statement was only one of many instances in which he told investors the digital transformation would be great for investors because it would be great for customers.

90. On a January 22, 2015 call to discuss Capital One's Q4 2014 earnings, Defendant Fairbank stated that:

> I think, in the long run, there's going to be [a] very significant cost benefit from all these digital investments, but the biggest benefit, and the reason we're doing it is, in almost all cases, not for that reason. And what I'm most excited about is actually the opportunities to generate growth and to generate better real-time decision-making, to make better credit decisions, and in the end build a deeper franchise through very significant improvements

> in the customer experience and things that really create more loyalty and more stickiness with customers.

91. On a July 23, 2015 call to discuss Capital One's Q2 2015 earnings, Defendant Fairbank stated that "[w]hile you can't necessarily see it in the numbers that you see, but the enhancements to productivity, the power of innovation, the dramatically growing customer experience benefits and it's inextricably linked to the growth that we are generating right now."

92. In a February 10, 2016 presentation at the Credit Suisse Financial Services Forum, Fairbank told investors that:

> The more important things, where I see such big opportunity, is ***the opportunity to really transform the customer experience***, to really change how we do marketing, to ultimately increasingly leverage the big data that is out there, increasing in a world of big data to leverage information to make smart decisions, to move over time through the world where a batch going to real time and a lot of dimensions that I think really help us grow and build a great franchise. And it's a shared path because along the way then there is a lot of savings to be had for those who do make the sustained investment.

93. In a November 30, 2016 presentation at the J.P. Morgan FinTech & Specialty Finance Forum, Jeff Norris noted that:

> Cost is an important thing, efficiency is an important thing, but in some ways it's almost the least important thing. ***We're also seeing better compliance outcomes, better and richer customer service and customer experience outcomes***, and productivity gains in terms of our speed of developing new software and new products and time-to-market. And I think the most obvious external benefit that we've seen thus far is the contribution to the industry-leading growth on our card business.

94. On an April 25, 2017 call to discuss Capital One's Q1 2017 earnings, Defendant Fairbank stated that "[t]he technology investments are not motivated first and foremost in order to save money, frankly, it's for a lot of the other benefits, ***that of a great customer experience***, the ability to transform how the business works, and so on."

95. On an April 25, 2019 call to discuss Capital One's Q1 2019 earnings, Defendant Fairbank stated that Capital One would not change much about how it had approached the digital transformation:

> Because we are absolutely compelled by the opportunity here. And we can feel the accelerating progress on just about every dimension. ***If you were inside this company, you could feel acceleration on what's happening with the customer experience, what's happening in risk management, what's happening with the dynamism of the company, the speed to market, the products, how customers are feeling about Capital One.***

96. And on a July 18, 2019 call to discuss Capital One's Q2 2019 earnings, Defendant Fairbank reiterated:

> And it is very clear inside our company and you're starting to see some manifestations externally that our tech progress is accelerating and the benefits which extend across a lot of different aspects of the business, from speed to market, to product quality, customer experience, risk management, operational effectiveness, growth efficiency, there's a lot of different aspects of it.

97. Thus, Defendants recognized that for the digital transformation to succeed, Capital One would have to employ its purported technological savvy to win and keep customers' loyalty.

98. Capital One acknowledged that it could not win and keep customers' loyalty unless it could keep customers' data safe. Capital One CFO Richard Blackley acknowledged at the Barclays Global Financial Services Conference on September 10, 2019, after the Data Breach, that "obviously, for a financial services firm, making sure that data is secure is a mission-critical thing[.]"

V. PRIVATE INFORMATION IS VALUABLE TO CRIMINALS

99. Identity theft is when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration date, and other information, without permission, to commit fraud or other crimes. Estimates put forth by the FTC are that as many as 10 million Americans have their identities stolen each year. Once identity thieves have private information, "they can drain your bank account, run up charges on your credit

cards, open new utility accounts, or get medical treatment on your health insurance."[4] So private information is "as good as gold" to identity thieves.[5]

100. Javelin Strategy and Research has stated that "1 in 4 data breach notification recipients became a victim of identity fraud."[6] Nearly half of consumers with a breached debit card became fraud victims within the same year.

101. Identity thieves can use private information to perpetrate many crimes. For instance, they may commit immigration fraud, obtain a driver's license or identification card in the victim's name, use the victim's information to secure government benefits, or file a fraudulent tax return with victim's information to obtain a fraudulent refund.

102. Criminals may also obtain medical services using consumers' compromised private information or commit other frauds, such as obtaining a job or procuring housing.

103. Accordingly, the risks associated with identity theft are grave. "While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[7]

---

[4] FTC, Signs of Identity Theft, available at http://www.consumer.ftc.gov/articles/ 0271-signs-identitytheft.

[5] FTC Interactive Toolkit, Fighting Back Against Identity Theft, http://www.dcsheriff.net/community/documents/id-theft-tool-kit.pdf.

[6] 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, http://www.javelinstrategy.com/brochure/276 (the "2013 Identity Fraud Report").

[7] True Identity Protection: Identity Theft Overview, http://www.idwatchdog.com/tikia//pdfs/IdentityTheft-Overview.pdf.

104. A 2008 Presidential Report on identity theft describes the protracted, harmful effects of such theft:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of nonfinancial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[8]

VI. CAPITAL ONE'S DIGITAL TRANSFORMATION NEGLECTS SECURITY

105. To support Capital One's Information Based Strategy, Defendants knowingly imperiled huge swaths of customer data.

106. The machine learning that Capital One was developing requires creating huge stores of data ("data lakes") and making them accessible within Capital One.

107. A company can responsibly limit the amount of data it makes accessible while implementing extremely strict controls on who could access the data. To do so, however, can slow down engineers who are attempting to develop new tools. It can also make machine learning algorithms less effective.

108. Contrary to Defendants' statements, Capital One abandoned basic cybersecurity requirements to improve the operational performance of its engineers and machine learning

---

[8] The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, at p.11 (April 2007), http://www.ftc.gov/sites/default/files/documents/reports/combating-identitv-theft-strategicplan/strategicplan.pdf.

algorithms. Capital One created data lakes far vaster than other banks' – for example, keeping credit card applicants' information from as far back as 2005. Capital One also tracked outcomes, including the successful applicants' credit limit, credit scores, balances, and payment history, thus providing hackers a roadmap of customers who can most profitably be targeted for identity fraud. Capital One also granted massively overbroad permissions to access this data. With so much noise from legitimate access to this data, Capital One would have great difficulty detecting any illegitimate attempts to access the data.

109. Ultimately, by sacrificing security to the needs of its developers and their algorithms for broad and quick access to data, Capital One made a catastrophic data breach inevitable.

A. More Data Makes Better Machine Learning Algorithms

110. Beginning in the 1990's, mathematicians began to make substantial breakthroughs in a theretofore-neglected branch of information theory: machine learning.

111. These mathematicians made critical discoveries in the early 2000's. These breakthroughs, coupled with the immense amount of data created by the internet, made industrial uses of machine learning possible.

112. Machine learning is an application of artificial intelligence through which systems can automatically "learn" and improve from experience without being explicitly programmed. For example, an algorithm might be given access to millions of pictures and told whether each of those pictures contained a human face. Through the millions of pictures and feedback, the program can learn patterns which can allow it to detect human faces.

113. Humans, however, excel at detecting human faces. Machine learning is most useful when used to detect patterns in areas where humans are not especially skilled. Many of these uses arise in the financial services industry.

114. For example, Capital One and other banks use machine learning to detect unauthorized use of credit cards. Provided with the history of millions of users' credit card transactions - including unauthorized transactions - a machine learning program can learn patterns suggestive of unauthorized transactions. With additional information from the users' own transaction history, the program can detect transactions which might be unauthorized. The bank can then prompt the user to confirm the transaction.

115. Machine learning requires data. There is a direct correlation between the amount of data provided to the machine learning algorithm and the effectiveness of machine learning algorithms. Thus, the more data Capital One makes available to its machine learning programs, the more accurate – and therefore useful – those programs will be.

116. Capital One also employs machine learning for various other tasks. Among many other examples, Capital One uses machine learning programs working on vast information databases to create real-time, individualized advertisements to maximize the chances of successfully selling a product or service to a customer, and uses deep learning techniques using more than one hundred million credit card applications to make more informed credit decisions. The machine learning algorithms comb through disparate sets of data, for example transaction history, credit history, current events, general demographic data, along with many others, as well as response rates to different offers or default rates, to determine the likely success rate of different offers or credit strategies for individual customers.

117. To enable more effective machine learning, vast data lakes must be organized and accessible to the machine learning algorithms. Thus, to power machine learning, Capital One had to create data lakes and make their data accessible. The more data Capital One placed in the data lakes, the better its machine learning algorithms would be; the more machine learning algorithms

Capital One granted access to the data lakes, the more specialized algorithms Capital One would have.

118. Defendants could have compromised between the need for high-performing programs and data security. Or Defendants could have instituted simple data protection techniques. But as more fully set out below, contrary to their statements that the digital transformation would improve all aspects of Capital One's business, including cybersecurity, every time Defendants had to choose between better-performing machine learning programs and data security, it chose machine learning. As a result, a breach of the data lake was inevitable. Because the data lakes were enormous, if Capital One were hacked by criminals out for profit, any breach would be catastrophic.

B. Capital One Created Too Many Data Lakes and its Data Lakes Were Overbroad

119. To empower its machine learning programs, Capital One created huge data lakes.

120. In the Data Breach, the hacker was able to access a data lake containing the personal information of persons who had applied for credit cards as far back as 2005.

121. Storing data from as far back as 2005 would have provided useful information for Capital One's machine learning algorithms. It would have allowed them to learn how applicants who received credit in the flush years of the mid 2000's would perform during the Great Recession. This information would help Capital One make decisions about extending credit today when credit is again relatively easy.

122. Further, to support its machine learning algorithms, Capital One included credit outcomes alongside the customers' personally identifying information. These include the customers' financial data, such as income, credit limits, credit scores, and payment history. By including information about the ultimate results, Capital One allowed its algorithms to determine whether any particular extension of credit was successful – and thereby to discern patterns about

applicant characteristics that are indicative of success. In essence, keeping the data lakes the way they were allowed Capital One to teach its algorithms to identify not only poor credit risks but also "heavy spenders."

123. But customers who score high on these metrics are ideal targets for identity fraud, since fraudsters will be able to use their information to take out larger loans or larger amounts of credit, apply for larger tax refunds, or the like. Thus, not only did Capital One store the data necessary for fraudsters to commit identity fraud, it identified exactly which customers' identities were the most worth stealing.

124. The sole purpose of these vast and insecure data lakes was to enhance machine learning.

125. Capital One's retention of data far exceeds customers' reasonable expectations of how their data would be used. Customers applying for a credit card in 2005 would not imagine that their personal information would still be stored and used fourteen years later, alongside later years' financial information.

126. By keeping so much data and pointing out to hackers exactly how to use the data, Capital One ensured that any data breach by criminals intent on the fraudulent use or sale of personal information would be catastrophic.

127. Moreover, according to FE 1, while FE 1's division was in charge of creating the cloud security infrastructure, Capital One delegated authority for security to individual lines of business (e.g. credit cards, auto loans, commercial credit), thus permitting each line of business to create its own massive data lakes

128. The data lake whose data was stolen by the hacker responsible for the Data Breach was plainly created by the credit card division. But as FE 1's report shows, Capital One's other divisions also created their own data lakes, each of which was a vulnerability.

129. Compounding the problem, FE 2 reported that Capital One did not have a map of its internal network. Capital One had acquired numerous banks and tech companies. Capital One had granted these acquired companies access to its network but had not retired the companies' own network. Thus, Capital One's network was large and hazardous. Yet Capital One never created a complete map of its network.

130. Moreover, according to FE 2, Capital One had acquired numerous data lakes as a result of its many acquisitions. In fact, when Capital One acquired a company, it was more likely than not that it would not incorporate the data lakes into its network map. Capital One had many data lakes it did not even know existed.

C. Capital One Granted Access to the Data Lakes Far Too Easily

131. When guarding sensitive information, any person with access is a potential data thief. Thus, it is a widely-accepted basic cybersecurity principle that companies should limit users to the level of permissions necessary to do their jobs ("least privilege principle").[9] The least privilege principle is enshrined in several cybersecurity best practices Capital One claimed to follow.

132. According to FE 1, not only would individual lines of business create their own data lakes, they were also responsible for creating their own security protocols and access controls.

---

[9] For example, an industry publication put out by an organization which counts Capital One as a member explains: "The more people who have access to cardholder data, the more risk there is that a user's account will be used maliciously." *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures.*

Individual lines of business decided to whom to grant access to their data lakes. Individual lines of business were also responsible for insuring that "access aligned with responsibilities" of the parties seeking access to data.

133. FE 1's group was responsible for creating and implementing Capital One's data security infrastructure. According to FE 1, the infrastructure FE 1 created was like a building; the lines of business were like tenants. According to FE 1, each tenant was in charge of creating and managing its own plumbing, electrical systems, and the like. This creates substantial risks, as different tenants will have different preferences as to necessities.

134. The resulting security controls were chaotic. Even assigning responsibility for the Data Breach is difficult, FE 1 said, because "so many parties are involved."

135. Leaving each division responsible for its own security would clearly have benefited Capital One's programming and machine learning. By streamlining the process of obtaining access controls, Capital One made it easier for the lines of business to grant wide access to facilitate more rapid development. Further, by placing access controls in the hands of persons who reported to the heads of lines of business who were evaluated based on their business lines' operations – rather than to a CISO whose primary responsibility was data security – Capital One ensured that the access controls would prioritize operational effectiveness over security.

136. After the Data Breach, technology journalists Rob Wright and Chris Kanaracus published an August 5, 2019 article reporting on a conversation with a former Capital One cybersecurity employee. The employee was quoted as saying that Capital One's practice was to set overbroad access:

> Setting permissions can be tricky, too. You may be in a rush to push out code, and if you set permissions that are too narrow, you'll be flooded with troubleshooting requests. So what ends up happening is you set wider permissions and greater access than is necessary.

137. Indeed, between 2017 and 2019, there were four separate incidents in which Capital One insiders used overbroad permissions to improperly access ***multiple*** customers' personal information. Capital One was responsible for more insider breaches than any other bank. See ¶220, below.

138. FE 2 reports that compared to his government and subsequent private practice experience, Capital One's cybersecurity was "lackadaisical."

139. FE 2 reports one example of Capital One's recklessness with personal data. In September 2016, Yahoo Inc. announced that it had suffered a data breach which exposed 500 million Yahoo accounts. FE 2's superior hired a company closely connected with the Russian government and intelligence agencies ("Russia-Affiliated Vendor") to illegally purchase the breached data on the Dark Web.

140. Capital One then stored the stolen Yahoo usernames and passwords on its own server in a searchable plaintext spreadsheet. Capital One did not encrypt the usernames and passwords in any way. Thus, anyone with access to the server could access the usernames and passwords. Yahoo usernames were displayed to anyone who corresponded with the user. Thus, any one of Capital One's then-47,300 employees could search the spreadsheet for the usernames of ex-lovers, persons against whom they had a vendetta, or persons about whom they were curious, and obtain access to their email. To FE 2's knowledge, the database was not taken down while he was employed by Capital One.

141. FE 2 also reports that his superior had also hired the Russia-Affiliated Vendor for a regular contract. To obtain the Russia-Affiliated Vendor's services, Capital One employees logged directly onto the Vendor's website without using a virtual private network (i.e., a VPN).

The manner in which Capital One used these services also gave this Vendor access to Capital One's server and the data contained therein.

142. From his previous government experience, FE 2 was aware of classified and unclassified information raising counterintelligence concerns about the Russia-Affiliated Vendor. Further heightening FE 2's concerns, the Russia-Affiliated Vendor had asked Capital One, and been asked by Capital One, unusual questions of a political nature. In December 2016, FE 1 provided the unclassified information to his superior and raised his counterintelligence concerns in a four- to six-page memo. In a March 2016 meeting, FE 2 and FE 2's colleague (a retired FBI agent with 24 years' experience) urged FE 2's superior to terminate the contract with the Russia-Affiliated Vendor. FE 2 and FE 2's colleague offered to have certain of their former colleagues who still worked for the government provide an unclassified briefing. Instead, FE 2's superior ordered FE 2 and his colleague not to disclose anything about the contract to the government. An unrelated meeting between FE 2 and certain government employees was cancelled.

143. Alarmed by FE 2's superior's response, FE 2 sent the memo he had written along with a summary of the dispute to Capital One's human resources department. FE 2 also told Capital One's human resources department about the plaintext Yahoo username and passwords on Capital One's server. FE 2 was put in touch with a separate department within human resources with internal security audit functions, which handled his complaint.

144. Yet even as FE 2's complaint was "investigated", FE 2's superior pressured FE 2's colleague into approving the renewal of the contract with the Russia-Affiliated Vendor. The contract was in fact approved. No approval from Capital One's legal department or anyone else was sought or obtained.

145. In retaliation for FE 2's memo and complaint, FE 2's superior placed FE 2 on probation. Capital One eventually pushed out both FE 2 and FE 2's colleague. The contract with the Russia-Affiliated Vendor was not terminated.

D. Capital One's "Lackadaisical" Security and Multiple Security Breaches Created an Environment Where Employees Could Easily Miss Impermissible Transfers

146. According to FE 1, individual lines of business were also responsible for monitoring their networks for unusual uses of data that might be data breaches.

147. According to FE 1, a competent network should have been able to detect when the hacker exfiltrated large amounts of data from Capital One's server.

148. By granting access to so many individuals and machine learning programs, Capital One created so many sources of legitimate data requests that it was difficult to identify illegitimate data requests.

149. Moreover, Capital One suffered near-constant cybersecurity attacks and data breaches. According to FE 3, during his tenure, Capital One suffered upwards of 20 cyber attacks per month. According to FE 3, Capital One "didn't know what to do to prevent" cybersecurity incidents, and instead would "just hope" that any breach would "not be so bad."

150. FE 3 attended regular meetings with Defendant Johnson. In these meetings, FE 3 reported to Johnson data from his team about attacks on Capital One's server. FE 3 understands that in turn, these breaches were reported to Defendant Alexander.

E. Capital One's Encryption Did Literally Nothing to Stop Hackers from Obtaining "Encrypted" Data

151. Capital One protected its data behind a Web Application Firewall ("WAF"). A WAF is, in effect, a shield placed between a server and traffic originating from the Internet which aims to filter out malicious attacks.

152. A WAF uses programmed rules to distinguish between legitimate access requests, which it permits, and illegitimate access requests, which it denies.

153. If a request is legitimate, then the WAF automatically assigns the requester a role. These roles establish what portions of the server the requester will have access to as well as the conditions of that access. The requester receives temporary credentials assigned to that role.

154. If properly implemented, a WAF should deny access to all entrants except those who have already been approved. But Capital One's WAF was misconfigured, allowing access to malicious outsiders under certain circumstances.

155. Basic cybersecurity principles require multiple layers of defense. There are too many malicious actors to presume that a firewall will keep out all intruders.

156. Encryption is the second line of defense behind any firewall, including a WAF. Proper encryption ensures that if an intruder breaches the firewall, the intruder will only obtain unusable encrypted data.

157. But Capital One's "encryption" did no such thing. The credentials assigned with all roles automatically decrypted all data in the data lakes. Thus, merely bypassing the firewall gave an intruder unencrypted data. Since an intruder by definition bypasses the firewall, this meant that encryption was absolutely ineffective. It is akin to locking a door with two locks but having the same key open them both.

158. In announcing the Data Breach, Capital One defended itself by claiming that the method the hacker used to obtain access to the server decrypted the data.

159. Experts scoffed at Capital One's excuse.

160. John Bambenek, VP security research and intelligence at cybersecurity firm ThreatSTOP, was quoted in a July 30, 2019 Motherboard article as saying that Capital One's

"encryption is academic at best because if just a username and password is required, then for any threat model in effect there is no encryption."

161. A July 30, 2019 SC Magazine article quoted Jerry Ray, COO of SecureAge, as saying that "Capital One's claims regarding its encryption practices is weak. Particularly the line about, 'unauthorized access also enabled decrypting,' which goes against the very core function of responsible encryption practices. It's precisely when unauthorized attempts to access data occur that encryption displays its value and worth."

162. Other experts simply described Capital One's data as "unencrypted." An August 2, 2019 CIO Dive article reported remarks by M. David Peterson, cloud architect at MasterControl, that "Capital One made a mistake in not encrypting data." Peterson added that the decision was obviously wrong – "Why store anything on S3 unencrypted?"

163. Dylan Gilbert of the independent group Public Knowledge was quoted as saying "Why didn't Capital One fully encrypt this data, and why didn't the company place this vast trove of personal information behind a properly configured firewall?"

164. Once past the firewall, any user with Capital One credentials – a username and password – would have the data automatically decrypted by Capital One. Every hacker necessarily obtains credentials from the company to perpetrate the hack. Capital One's encryption was utterly pointless.

F. The Wall Street Journal Reports Internal Strife in Capital One's Cybersecurity Division

165. On August 15, 2019, the Wall Street Journal published an exposé, written by AnnaMaria Andriotis and Rachel Loise Ensign, about the Capital One culture which had led to the Data Breach ("August 15 Exposé"). The August 15 Exposé cited conversations with multiple persons with knowledge.

166. The August 15 Exposé recounted that Defendant Johnson clashed with Cybersecurity Division employees from the very beginning of his tenure as CISO. The cited sources reported that Johnson prioritized his own front office, which dealt with internal public relations, over the Cybersecurity Division's core operations.

167. The quality and experience of the Cybersecurity Division's employees is critical to Capital One's operations. In fact, Capital One's board regularly reviewed the Cybersecurity Division's attrition rates. Capital One's 2018 and 2019 Proxy Statements each provided that "[t]he Risk Committee receives regular quarterly reports from the Chief Information Security Officer on the Company's cyber risk profile and enterprise cyber program and meets with the Chief Information Security Officer at least twice annually."

168. Yet after Johnson's appointment, according to the sources cited in the August 15 Exposé, turnover in the Cybersecurity Division reached crisis levels. Most of Johnson's initial direct reports departed before the WSJ Article, as did many of their replacements. In total, about ***one third*** of the Cybersecurity Division's employees left in 2018 – a catastrophically high rate given that cybersecurity employees typically have far longer tenure than other information technology and computer science workers.[10]

169. Before the Data Breach, Capital One employees had raised concerns about staffing issues and other problems to the bank's internal auditors, human-resources department, and other senior executives.

---

[10] A 2017 survey reported that found that fewer than 1% of job-seeking cybersecurity professionals had been at their employer for less than 1 year. Hiring and Retaining Top Cybersecurity Talent, (ISC)^2, at 16, available at https://www.isc2.org/-/media/Files/Research/ISC2-Hiring-and-Retaining-Top-Cybersecurity-Talent.ashx

170. Capital One neglected routine cybersecurity measures. For example, in late 2017, Capital One purchased software from a company called Endgame to improve its ability to detect data being exfiltrated in Data Breaches. But more than a year after buying the software, Capital One still had not finished installing it. The issue was flagged to Defendant Johnson.

VII. LOSS CAUSATION

A. A Hacker Steals 106 Million Credit Card Applicants' Unencrypted Data

171. On March 12, 2019, hacker Paige Thompson (who went by the username "erratic" on social media) gained access to a server containing one of Capital One's vast data lakes.

172. Because Capital One granted access promiscuously, by merely accessing the server, Thompson gained access to a vast data lake. The data lake contained data from fifteen years of individual and small business credit card applications made in the U.S. and Canada. Each individual entry listed the applicant's name, address, telephone number, email address, date of birth, last four digits of social security numbers, and estimated income. There were 106 million individuals affected. In addition, the data lake contained about one million Canadian applicants' Social Insurance Number, Canada's equivalent to social security numbers.

173. Thompson acted alone. She was not assisted by any Capital One employee or any others.

174. After obtaining access to the server, on March 22 and 23, 2019, Thomson used a command to list all the resources she had obtained access to. Thompson did so again on or about April 21, 2019.

175. The data contained in the data lake were not meaningfully encrypted. By obtaining access to Capital One's servers, Thompson was assigned credentials that automatically decrypted all the data available in the data lake.

176. Capital One tokenized most applicants' social security numbers and bank account numbers – i.e., replaced them with an undecipherable token referring to the original stored in a secure data vault. Yet 140,000 applicants' social security numbers and 80,000 customers' bank account numbers in the data lake were not tokenized. Thompson obtained these social security numbers and bank account numbers, too. The Canadian applicants' Social Insurance Numbers were also not tokenized.

177. The data Thompson gained access to also included, for each customer, the customer's status data, consisting of (for example) credit scores, credit limits, balances, payment history, and contact information. The data lake linked these data to the applicants' personal identifying information. Using these data, Thompson could have identified those applicants who had high credit scores, high credit limits, and high balances, precisely the kind of customers' information that is highly valued by criminals because their identities are the most profitable to steal. By linking financial information to Capital One customers' personal information, Capital One made the leaked data orders of magnitude more valuable to criminals. Guaranteed a high return if they are successful, criminals, in turn, were much more likely to "invest" in committing identity theft. Thus, Capital One's Data Breach could have proven every bit as destructive as the Equifax breach.

178. Thompson also obtained transaction data from a total of 23 days during 2016, 2017, and 2018. Thompson could have identified embarrassing transactions and used the information to blackmail customers.

179. On April 21, Thompson exfiltrated the data to outside of Capital One's firewall.

B. Capital One Does Not Learn of the Data Breach Until It Is Informed That the Hacker Had Publicly Bragged About It

180. Thompson's entries into Capital One's public cloud, and her actions therein, were recorded in Capital One's computer logs. Reviewing computer logs for suspicious actions is a fundamental principle of cybersecurity. But amid the chaotic requests made by Capital One's complex machine learning algorithms and multiple user accesses, Thompson's access was missed.

181. Indeed, Thompson was also able to employ Capital One's computing power to mine bitcoins without alerting Capital One. Mining bitcoins required extensive day-to-day unauthorized use of Capital One's computing power.

182. Capital One did not detect Thompson's entry, did not detect her copying the data, and did not detect that she was using Capital One's computer power to mine bitcoins.

183. On June 18, Thompson said on a private slack channel that she had obtained Capital One customers' social security numbers, full names, and dates of birth. On July 17, a member of the private slack channel reported the Data Breach to Capital One, along with the specific code Thompson had employed to breach Capital One's firewall.

184. Capital One then determined that its computer logs reflected Paige Thompson's hacking of its servers set out in ¶¶172, 176-78, above.

C. Capital One Only Escaped Catastrophic Harm Because It Was Incredibly Lucky

185. Had Capital One been hacked by a conventional team, the ramifications would have been catastrophic. Because Capital One's data identified which customers criminals should target, the data would have fetched exorbitant prices on the dark web. Criminals would have eagerly cashed in on their purchase by stealing high-value customer' identities. By increasing the average payoff for a successful theft, Capital One would have ensured that a far higher proportion of customers whose data was leaked would have their identity stolen. Meanwhile, criminals would

have attempted to blackmail Capital One customers who had embarrassing transactions. The leak would have gone undetected until the data was already sold, because conventional criminal hacking teams keep quiet about their crimes.

186. Yet Capital One was not hacked by a conventional team. It was hacked by Thompson – a disturbed individual acting alone who had no plans to monetize her theft and got caught because she boasted of the hack.

187. As Blackley acknowledged at the Barclays Global Financial Services Conference taking place on September 10, 2019:

> And our investigation concluded that the individual was basically hacking to steal computing power and that the purpose for that was crypto mining rather than looking for personal data for fraud. It's now been a month since the arrest happened, and the US Attorney's Office has continued to investigate after the arrest. And they actually announced during the bail hearings in August that they believed that they have recovered the only copy of the data and that they see no evidence that the data was used for fraud, that it was sold or otherwise disseminated. They also indicted the perpetrator two weeks ago, and no changes were brought -- or no charges were brought around fraudulent use of the data. So we're in a slightly different situation of having data that wasn't -- while it was accessed, it appears that it was not released or used for fraud in any way. ***I think that makes this situation a bit unique.***

188. Had the Capital One hacker been a conventional hacking team, Capital One might have suffered billions of dollars in damages. Through sheer dumb luck, while the Data Breach revealed that Defendants' statements were false, Capital One never suffered the catastrophic harm these statements concealed.

D. Capital One's Announcement of the Data Breach Shocks the Market

189. On July 29, 2019, after trading closed, Capital One issued a press release announcing that: (a) it had suffered a data breach; (b) the hacker had stolen 106 million credit card applicants' data; (c) the stolen data consisted of the data set out in ¶¶¶¶172, 176-78, above. Yet in the press release, Capital One also reassured investors that "[b]ased on our analysis to date, we believe it is unlikely that the information was used for fraud or disseminated by this individual."

190. On July 30, 2019, the price of Capital One's shares fell 5.9% on heavy volume from its previous close of $96.92 to $91.21, damaging investors.

191. In its press release announcing the data breach, Capital One estimated that it would spend $100 million to $150 million in 2019 alone on remediation. As of around October 4, 2019, Capital One employees in its tech and cyber departments had spent 200,000 hours responding to and remediating the Data Breach.

192. Analysts who had been repeatedly told by Capital One about its tech savvy were surprised that the Data Breach had occurred:

a. A July 29, 2019 J.P. Morgan report stated that "We note, however, that [Capital One] has been an industry leader in moving towards cloud-based service […] While it is unclear whether this is directly related to [Capital One]'s transition to a cloud-based infrastructure, we believe this will be a renewed concern going forward."

b. A July 30, 2019 Morgan Stanley report stated that the "Cyber incident raises questions on how best to police and protect client information. Capital One has not been shy about its journey towards a 100% cloud model, which comes with today's period of leveraging Amazon Web Services. Today's revelation reminds investors of the trust that financial institutions place in their client-facing employees and highlights risks of outsourcing any part of client-facing operations."

c. A July 30, 2019 Credit Suisse report stated that "[S]ince [Capital One] has been vocal about the importance of financial institutions migrating to the cloud, investors may now have questions on the vulnerability of such infrastructure[.]"

d. A July 29, 2019 RBC report stated that "We want to be fair and balanced in our thinking on the stock, but it is a tough headline and there are likely some challenging public and political pressures ahead."

193. Security experts were likewise shocked that Capital One fell prey to such an unsophisticated attack. John Dickson, a security professional with security consulting firm Denim Group, was quoted in a July 31 article as saying that "[t]he biggest surprise is the amateur nature of the attack," adding that it was "absolutely earth-shattering" that the attacker obtained so much data so easily.

194. In addition to financial losses, Capital One suffered substantial reputational harm. A bank like Capital One must prove to customers that the bank will maintain their private data with the strictest security. Customers trust their banks with critical information, including social security numbers. Customers provide banks with deeply personal information like their income, their indebtedness, and their purchases. Customers rightly fear that criminals who obtain their bank information will be able to directly cause them financial harm.

195. Defendant Fairbank acknowledged *before* the data breach that Capital One had a critical competitive advantage because while customers do not necessarily expect such care from tech companies, they do expect that banks will keep their data safe. See ¶241, below. By exposing how much Capital One's business plan depended on loosening security restrictions, news of the data breach gave customers a reason to find a bank which is not cavalier with their data.

196. In an August 13 letter to Senator Ron Wyden, Amazon Web Services stated that it offered ***three*** services that would have prevented or rapidly detected the hack.

197. In November 2019, the Wall Street Journal reported that Capital One fired Defendant Johnson because of the Data Breach.

198. The Data Breach spurred investigations by a dozen state Attorneys General and the House Committee on Oversight and Reform. In addition, Capital One faces at least 70 consumer class actions over the Data Breach, filed in both the U.S. and Canada.

VIII. DEFENDANTS' FALSE AND MISLEADING STATEMENTS

A. Capital One's Legal Obligations and Industry Practices

199. The U.S., individual states, and foreign countries in which Capital One did substantial business regulate its conduct regarding protection for and use of data.

200. The Gramm-Leach-Bliley Financial Services Modernization Act of 1999 ("GLBA") requires financial institutions to "protect the security and confidentiality" of the personal information they collect by, among other things, "develop[ing], implement[ing], and maintain[ing] a comprehensive information security program" that "contains administrative, technical, and physical safeguards that are appropriate to [the] size and complexity [of the financial institution], the nature and scope of [its] activities, and the sensitivity of any customer information at issue" ("Safeguards Rule"). The Federal Trade Commission, responsible for enforcing the Safeguards Rule, has issued guidance and published regulatory decisions interpreting the measures financial institutions must take to comply with the Safeguards Rule.

201. In its interpretation of the Safeguards Rule, the FTC recommends:

a. Limiting access to customer information to employees who have a business reason to see it.

b. Know where sensitive customer information is stored and store it securely.

   i. When customer information is stored on a server or other computer, ensure that the computer is accessible only with a "strong" password and is kept in a physically-secure area.

   ii. Where possible, avoid storing sensitive customer data on a computer with an Internet connection.

iii. Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored.

202. The FTC has interpreted Section 5 of Federal Trade Commission Act ("FTC Act"), barring "unfair or deceptive acts or practices", to encompass failures to appropriately store and maintain personal data. The body of law created by the FTC recognizes that the following conduct may violate the FTC Act:

a. Citing the National Research Council, the FTC has concluded that "[p]rocedures should be in place that restrict users' access to only that information for which they have a legitimate need."[11] Failure to segregate access may violate FTC Act.

b. Failure to use "readily available security measures [] to limit access between and among" various data storage systems.[12]

c. Providing nearly all employees ability to exercise administrative control and obtain personal information.[13]

203. Capital One did substantial business in Canada, whose Canadian Model Code for the Protection of Personal Information mandates the implementation of safeguards to protect information in proportion to its sensitivity. These safeguards include "limiting access on a 'need to know' basis" and "the use of passwords and encryption."

204. The PCI (Payment Card Industry) Security Standards Council, which counts Capital One as a member, has published its *Payment Card Industry (PCI) Data Security Standard:*

---

[11] *In the Matter of LabMD, Inc.*, Dkt. No. 9357, Slip Opinion, at 15, available at https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf.
[12] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 258 (3d Cir. 2015).
[13] *In the Matter of Twitter, Inc.*, 151 F.T.C. 162, 164 (2011).

Requirements and Security Assessment Procedures ("Requirements"), the latest version of which is dated May 2018.

205. Capital One violated the Requirements' mandates concerning data retention, encryption, and access.

206. Capital One's unreasonably long retention periods violated the Requirements' mandates on data storage, which command in relevant part:

a. Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data [] storage:

    i. Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements.

207. By automatically decrypting data for entrants, Capital One violated the Requirements' mandates on encryption and access, which command in relevant part:

a. Restrict access to cryptographic keys to the fewest number of custodians necessary.

b. Store cryptographic keys in the fewest possible locations.

c. Secure cryptographic key distribution.

d. Secure cryptographic key storage.

e. Limit access to system components and cardholder data to only those individuals whose job requires such access.

f. Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed [including] [a]ssignment of privileges to individuals based on job classification and function.

g. Encrypt all non console [local computer] administrative access using strong cryptography.

h. Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.

208. Capital One's 2015, 2016, 2017, and 2018 10-Ks,[14] each of which was signed by Defendant Fairbank, each provided that:

> ***Compliance Risk Management***
>
> We recognize that compliance requirements for financial institutions are increasingly complex and that there are heightened expectations from our regulators and our customers. In response, we continuously evaluate the regulatory environment and proactively adjust our compliance risk program ***to fully address these expectations***.
> Our Compliance Management Program establishes expectations for determining compliance requirements, assessing the risk of new product offerings, creating appropriate controls and training to address requirements, monitoring for control performance, and independently testing for adherence to compliance requirements. The program also establishes regular compliance reporting to senior business leaders, the executive committee and the Board of Directors.
> The Chief Compliance Officer is responsible for establishing and overseeing our Compliance Risk Management Program. Business areas incorporate compliance requirements and controls into their business policies, standards, processes and procedures. They regularly monitor and report on the efficacy of their compliance controls and Corporate Compliance periodically independently tests to validate the effectiveness of business controls.
> (first emphasis in original)

209. Each of the 10-Ks defines compliance risk as "the risk to current or anticipated earnings or capital arising from violations of laws, rules, or regulations. Compliance risk can also arise from ***nonconformance with prescribed practices, internal policies and procedures, contractual obligations, or ethical standards that reinforce those laws, rules, or regulations***[.]"

[14] Filed, respectively, on February 25, 2016, February 23, 2017, February 21, 2018, and February 20, 2019.

210. Capital One's Online & Mobile Privacy Statement, available on its website throughout the Class Period, advised Capital One customers in relevant part:

> At Capital One, we make your safety and security a top priority and are committed to protecting your personal and financial information. If we collect identifying information from you, ***we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices***.

211. The emphasized statements in this section were false and misleading because they gave investors the misleading impression that with respect to cybersecurity Capital One had met and exceeded: (a) regulatory requirements; (b) customer expectations; and (c) industry best practices. In truth, defendants knew or were reckless in not knowing that Capital One was sacrificing cybersecurity by creating dangerously large data pools, granting widespread access, and failing to monitor data requests, as more fully set out in ¶¶105-170, above; and violating a host of industry practices and ethical standards, as set out in ¶¶105-170, above.

B. Defendants Violated Regulatory Obligations To Disclose Information About the Risks Created By Capital One's Cybersecurity Policies

212. In October 2011, the SEC provided guidance on disclosure of cybersecurity risks ("2011 Guidance"). In the 2011 Guidance, the SEC informed companies that "[r]egistrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky." Disclosure should include "[d]iscussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences." Companies should also "address cybersecurity risks and cyber incidents in their MD&A if the costs or other consequences associated with [] the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition."

213. On February 21, 2018, in the wake of several high-profile data breaches, the SEC issued its *Statement and Guidance on Public Company Cybersecurity Disclosures*, Release Nos. 33-10459; 34-82746 ("2018 Guidance").

214. The purpose of the 2018 Guidance is to provide the SEC's views on issuers' obligations to disclose material cybersecurity risks.

215. In the 2018 Guidance, the SEC emphasized that "it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, ***including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.***"

216. In the 2018 Guidance, the SEC explained that it:

> Expect[s] companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents. As the Commission has previously stated, we 'emphasize a company-by-company approach [to disclosure] that allows relevant and material information to be disseminated to investors without boilerplate language or static requirements while preserving completeness and comparability of information across companies.' Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.

217. Capital One CFO Richard Blackley acknowledged at the Barclays Global Financial Services Conference on September 10, 2019 that "obviously, for a financial services firm, making sure that data is secure is a mission-critical thing[.]"

218. In each of Capital One's 2015-2018 10-Ks, Defendants warned identically of cybersecurity risks. These disclosures were not tailored to Capital One, but instead applied to any company with large amounts of data and any financial services firm.

219. In the 2018 Guidance, the SEC also stated that:

> In meeting their disclosure obligations, companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of these risks in the appropriate context. For example, if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur.

> Instead, the company may need to discuss the occurrence of that cybersecurity incident and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose particular risks to the company's business and operations.

220. Montana law requires that businesses notify its Office of Consumer Protection whenever a Montanan's personal information is compromised. The Office of Consumer Protection posts all such notices on the Montana Department of Justice's website. See https://dojmt.gov/consumer/databreach/. Between 2017 and the Data Leak, there were four separate incidents in which Capital One insiders used overbroad permissions to improperly access more than one Montana Capital One customer's information:

a. Between January 2017 and April 2017, a former Capital One employee improperly accessed Montana Capital One customers' personal information;[15]

b. As reported in a June 18, 2018 sample letter, at an unspecified time, another former employee again accessed Montana Capital One customers' bank account information;[16]

c. Between June 9, 2018, and July 23, 2018, a former employee of a Capital One service provider accessed Montana Capital One customers' personal information;[17]

d. Between December 1, 2018, and April 19, 2019, a former Capital One employee accessed Montana Capital One customers' personal information.[18]

221. No other bank had close to as many insider breach incidents during this period, or even cybersecurity incidents of any kind.

---

[15] https://media.dojmt.gov/wp-content/uploads/Capital-One-2-1.pdf
[16] https://media.dojmt.gov/wp-content/uploads/Capital-One-6.2018-notification.pdf
[17] https://media.dojmt.gov/wp-content/uploads/Capital-One-5.pdf
[18] https://media.dojmt.gov/wp-content/uploads/Consumer-21.pdf

222. Capital One's 10-Ks were knowingly or recklessly false and misleading, as more fully set out in ¶¶105-170, above, for omitting to disclose that (a) Capital One was sacrificing cybersecurity by creating dangerously large data pools, granting widespread access, and failing to monitor data requests, and (b) Capital One faced a "particular risk" from overbroad access granted to presumed insiders.

C. Defendants Falsely and Misleadingly Stated that Capital One's Digital Transformation Was A Shared Path Which Led to Better Cybersecurity

223. Defendants made clear that the digital transformation to which they purportedly dedicated so much of Capital One's resources was a "shared path" which led to better cybersecurity. As Defendant Fairbank claimed on a call to discuss Capital One's Q3 2018 earnings taking place on October 23, 2018:

> [W]hat I am struck by [] and I'm not surprised by it, because I believe that that will accelerate here is that ***going all-in on this transformation is the opportunity to be way faster to the market, offer way better products, have way better risk management along credit dimensions, fraud, cybersecurity, that's all a shared path, same thing.*** Better operating controls in a world where the regulatory requirements and frankly the expectations on banks to deliver well-controlled environment in a complex industry is very, very high, better economics, and all of this in service of the most important thing, which is real-time, personalized experience for our customers, not just in an app, but integrated right into their lives. So that's the journey we're on.

224. This statement was one of several Class Period statements in which Defendants gave the misleading impression that Capital One's digital transformation included cybersecurity.

225. Norris told investors and analysts at the J.P. Morgan FinTech & Specialty Finance Forum on November 30, 2016 that because of the digital transformation, Capital One was "also seeing better compliance outcomes."

226. At the June 1, 2017 Sanford C. Bernstein & Co. Strategic Decision Conference, Defendant Fairbank stated:

> So what we've done over this period of time is to build out the capability of fully digital consumer banking and with a very robust checking account capability, ***all the fraud***

> ***defenses that go along with digital banking***, which by the way are significant, because fraudsters by the way don't go walking into local banks. They go set up checking accounts, they like to do all this stuff online.

227. As Capital One CFO Stephen S. Crawford explained at the J.P Morgan Fintech & Specialty Finance Forum on December 2, 2015:

> <Q>: The second part of the question is – and you've talked again about your technology spending, it's something that we have heard across the industry and one of the things that we haven't head as people talk about this, but we kind of wonder of underneath the surface, is this one of the things that's going on. How much of this is really devoted to cyber security and how big a concern is cyber security?
>
> <Crawford>: ***Cyber [security] is an important part of the overall digital process and you I think as a financial institution trust, the trust of our customers is critical, and we want to make sure that we're a leader in cyber, so it's one of the agenda items we have in the whole digital space.***

228. In a presentation at the June 15, 2016 Morgan Stanley Financials Conference, Crawford listed, as examples of aspects of Capital One's business that would benefit from the digital transformation "customer service, account acquisition, risk differentiation, ***regulatory compliance – there's not a single major undertaking or challenge the business has where, if you sit back and think about the implications of being able to deploy to the cloud or big data or open source software, they can't make a huge difference in both the revenue and the expense side.***"

229. Capital One's proxy statements also treated its digital transformation and cloud security in the same breath. For example, Capital One's 2018 Proxy Statement, filed with the SEC on March 20, 2018, sent on behalf of the Board of Directors that Fairbank chaired, provided that in 2017 Capital One's management had "[a]ccelerated focus on cloud capabilities, modern software engineering and delivery, ***and enhanced cybersecurity capabilities.***"

230. The emphasized statements in this section were false and misleading because, knowingly or with reckless disregard, Defendants misled investors: (a) by including cybersecurity with what Defendants described as Capital One's epochal digital transformation, Defendants gave

the misleading impression that Capital One was making cybersecurity a priority, when in truth, as more fully described in ¶¶105-170, above, Capital One was sacrificing cybersecurity by creating dangerously large data pools, granting widespread access, failing to monitor data requests, and failing to meaningfully encrypt data; (b) the statements gave the misleading impression that Capital One's digital transformation was improving cybersecurity, when in fact the digital transformation required Capital One to abandon basic cybersecurity practices, as more fully described in ¶¶105-170, above; (c) the statements gave the misleading impression that cybersecurity and the benefits Capital One claimed from its digital transformation went hand in hand, when in truth because of Capital One's business plan emphasizing the change to machine learning in its digital transformation, in order to maximize machine learning capabilities Defendants compromised cybersecurity, as more fully described in ¶¶105-170, above; and (d) defendants omitted to disclose that by not protecting Capital One's customers personal data, Capital One exposed customers to much ***more***, not less, serious risks of fraud, as more fully described in ¶¶105-170, above.

D. Defendants Claimed Cybersecurity Was One of Capital One's Top Priorities

231. Defendants repeatedly made statements touting Capital One's investments in cybersecurity.

232. In explaining the digital transformation during a July 23, 2015 call to discuss Capital One's Q2 2015 earnings, Defendant Fairbank stated:

> ***We're investing in cybersecurity. This is an incredibly important area and we are putting a lot of very top talent and a lot of energy and investment into that.***

233. On October 7, 2015, Defendant Alexander announced at AWS re:invent 2015, an industry convention, that Capital One would shift all of its operations and data to the cloud. In prepared remarks, Defendant Alexander stated:

> … ***security is critical for us.*** The financial services industry attracts some of the worst cyber criminals so we work closely with the Amazon team to develop a security model that

> we believe ***enables us to operate more securely in the public cloud than we can even in our own data centers.***

234. On June 25, 2019, at the AWS re:inforce conference, in prepared remarks, Defendant Johnson stated that:

> Cyber is evolving from a trade craft to a science and cyber professionals are defining the future of business.
>
> * * * * *
>
> ***Most important to us is the confidentiality, integrity and the availability of our data in the cloud. Cloud native companies must take a multi-layered approach to security***, leveraging internally developed tools like the Capital One-developed open source Cloud Custodian.

235. On November 21, 2018, Capital One EVP and CTO Brady, who led 4,000 Capital One employees, published an article on Capital One's website. Brady's article provided, in relevant part: "In an effort to help our application teams migrate to the cloud in an unencumbered way, we established a governance function with security and compliance as top considerations."

236. Capital One's 2015, 2016, 2017, and 2018 10-Ks provided that:

> We safeguard our customers' and our own information and technology, implement backup and recovery systems, and generally require the same of our third-party service providers. ***We take measures that mitigate against known attacks and use internal and external resources to scan for vulnerabilities in platforms, systems, and applications necessary for delivering Capital One products and services***.

237. In Capital One Press Releases dated October 31, 2017, December 5, 2017, January 24, 2018, announcing Capital One collaborations, Rebecca Hieronimous, Capital One's Vice President of Enterprise Digital Products and Data Connections, was quoted as saying "We know many of our customers actively use the [product at issue] and we are excited to enable this partnership allowing customers to share their data in a way that is ***secure, transparent and under their control***."

238. Since at least September 29, 2018, Capital One's cybersecurity policy, available on its website, has stated at the top of the page in roughly 33-point font that "Your security is a top priority".[19]

239. The foregoing statements were false and misleading because, knowingly or with reckless disregard: (a) Defendants gave the misleading impression that cybersecurity was a "top", "critical", "most important", or "incredibly important" priority for Capital One, when in truth, Capital One was sacrificing cybersecurity by creating dangerously large data pools, granting widespread access, failing to monitor data requests, and failing to meaningfully encrypt data, as more fully set out in ¶¶105-170, above; (b) Defendants gave the misleading impression that cybersecurity and the benefits Capital One claimed from its digital transformation went hand in hand, when in truth because of Capital One's business plan cybersecurity and the other benefits anticipated from Capital One's digital transformation were trade-offs; (c) because breaching Capital One's firewall also decrypted Capital One's data, Capital One's data was not secure and had only one layer of defense.

240. Throughout the Class Period, Defendants claimed that as a financial institution, Capital One faced and followed more stringent data security requirements than tech companies.

241. Defendant Fairbank explained at the Barclays Global Financial Services Conference taking place on September 11, 2017 that Capital One would outcompete tech companies because of its reputation for safeguarding customers' private information:

> Capital One is trying to build basically a tech company that happens to be a major player in banking and I really think the opportunity is great for players who do that. I think the journey is incredibly hard for banks to get there. The fact that we're regulated, huge capital requirements, the risk management involved in our business ***and even some of the brand credibility associated with the management of people's private information and their***

[19] https://www.capitalone.com/applications/identity-protection/commitment/

money are things that will help us slow banks possibly make our way successfully to the destination.

242. On a video posted to YouTube on August 24, 2018, Defendant George Brady, Capital One's Executive Vice President and Chief Technology Officer, was quoted as saying:

> ***As a financial institution, we take the safety of our customer data incredibly seriously.*** Before we moved a single workload, we engaged groups from across the company to build a risk framework for the cloud that met the same high bar for security and compliance that we meet in our on-premises environments.

243. Capital One's 2018 Proxy Statement provided:

> ***As a financial services company entrusted with the safeguarding of sensitive information, our Board believes that a strong enterprise cyber strategy is vital to effective cyber risk management.*** Accordingly, our Board is actively engaged in the oversight of the Company's cyber risk profile, enterprise cyber strategy implementation and key cyber initiatives. The Risk Committee receives regular updates from management on its cyber event preparedness efforts. The Risk Committee receives regular quarterly reports from the Chief Information Security Officer on the Company's cyber risk profile and cybersecurity program initiatives and meets with the Chief Information Security Officer at least twice annually. The Risk Committee also meets periodically with third-party experts, as appropriate, to evaluate the Company's cybersecurity program. The Risk Committee annually reviews and recommends the Company's information security policy and information security program to the Board for approval. The Risk Committee is also responsible for overseeing cybersecurity and information security risk as well as management's actions to identify, assess, mitigate and remediate material issues. At least annually, the Board reviews and discusses the Company's technology strategy with the Chief Information Officer and approves the Company's technology strategic plan.
>
> * * * * *
>
> ***[M]anagement continued to build risk identification and management capabilities, especially in the areas of cybersecurity, credit monitoring, and capital planning, and is committed to effective, proactive, and sustainable operation of these capabilities.***

244. Capital One's 2019 proxy statement, filed with the SEC on March 20, 2019 and sent on behalf of the Board of Directors that Fairbank chaired, provided:

> ***As a financial services company entrusted with the safeguarding of sensitive information, our Board believes that a strong enterprise cyber program is vital to effective cyber risk management.*** Accordingly, our Board is actively engaged in the oversight of the Company's cyber risk profile, enterprise cyber program and key enterprise cyber initiatives. The Risk Committee receives regular updates from management on its

> cyber event preparedness efforts. The Risk Committee receives regular quarterly reports from the Chief Information Security Officer on the Company's cyber risk profile and enterprise cyber program and meets with the Chief Information Security Officer at least twice annually. The Risk Committee also meets periodically with third-party experts, as appropriate, to evaluate the Company's enterprise cyber program. The Risk Committee annually reviews and recommends the Company's information security policy and information security program to the Board for approval. The Risk Committee is also responsible for overseeing cyber, information security, and technology risk, as well as management's actions to identify, assess, mitigate, and remediate material issues. At least annually, the Board reviews and discusses the Company's technology strategy with the Chief Information Officer and approves the Company's technology strategic plan. Additionally, the Risk Committee receives and reviews reports from the Chief Information Officer and the Chief Information Security Officer regarding significant cyber incidents impacting the Company, including management's assessment of the root cause and relevant learnings from the incident.
>
> * * * * *
>
> We continued to strengthen our risk and control environment and build risk identification and management capabilities, particularly in the areas of cybersecurity, credit monitoring and capital planning.

245. On May 20, 21, 22, or 23, 2019, Defendant Alexander spoke at the Collision Conference in Toronto, an event attended by 921 journalists and more than 850 Venture Capital firms and angel investors. Alexander stated that:

> We've been at the forefront of a pretty significant transformation. For example, you know, we are one of the furthest along in terms of actually migrating a legacy enterprise fully to the cloud. Along the way – and by the way, ***we've done that in an industry that is highly regulated, you know, sensitive data, security is paramount, and so we've had to really be thoughtful and careful, you know really invest in great engineering to make that journey work.***

246. The emphasized statements in this section were false and misleading because, knowingly or with reckless disregard, Defendants gave the misleading impression that Capital One had met and exceeded the regulatory requirements of and customer expectations concerning cybersecurity when in truth, Capital One was sacrificing cybersecurity by creating dangerously large data pools, granting widespread access, failing to monitor data requests, and failing to encrypt data, as more fully set out in ¶¶105-170, above.

E. Defendants Claimed that the Customer Data It Placed On Its Server was Effectively Encrypted

247. Defendants claimed that Capital One had encrypted the data it placed on the cloud and that this encryption provided a level of defense against infiltration by hackers.

248. In 2016, Capital One announced that one of its senior employees, Kapil Thangavelu had developed a new product it called Cloud Custodian. Mr. Thangavelu presented Cloud Custodian in multiple industry events. Most notably, Cloud Custodian was the subject of Mr. Thangavelu's keynote address at the AWS re:invent 2018 conference attended by tens of thousands of industry professionals, journalists, and other interested persons.

249. Capital One billed Cloud Custodian as a comprehensive cloud security tool which would automatically detect and fix security flaws. In particular, Defendants boasted that Cloud Custodian would automatically encrypt unencrypted data on Capital One's servers (or on any public cloud servers it leased).

250. On November 30, 2016, the Wall Street Journal's CIO Journal published an article titled *CIO Voices: Capital One's Rob Alexander on How to Win in Banking*, in which Defendant Alexander was quoted as saying:

> <Q> Is open source important?
> <Alexander> We're embracing open source for all of our new software and we contribute back to the community with our own products. We launched a tool called Cloud Custodian that we built to ensure that we encrypt all data that goes to the cloud. Cloud Custodian monitors our deployment in the public cloud to make sure all the things we deploy comply. ***If something's not encrypted, it will automatically encrypt it.***

251. On June 25, 2019, at the AWS re:inforce conference, in prepared remarks, Defendant Johnson stated that Capital One's cloud protections include "forced data encryption," referring to Cloud Custodian.

252. Capital One's 2015, 2016, 2017, and 2018 10-Ks, all of which were signed by Defendant Fairbank, provided that "[w]e believe we have a robust suite of authentication and

layered information security controls, including our cyber threat analytics***, data encryption and tokenization technologies***, anti-malware defenses and vulnerability management program."

253. Capital One's annual privacy notice to credit card holders stated "[t]o protet your personal information from unauthorized access and use, we use security measures that comply with federal law. ***These measures include*** computer safeguards and ***secured files*** and buildings."

254. The foregoing statements, issued knowingly or with reckless disregard, were false and misleading. In fact, as described more fully at ¶¶105-170, above: (a) Capital One's overbroad granting of permissions, adopted to further its digital transformation, allowed any user with a Capital One username and password to decrypt data lakes; (b) by necessity, any user who breached Capital One's firewall would be assigned a Capital One username and password; and (c) as a result, even if Capital One did encrypt data on its server, such encryption was no encryption at all because any successful breach of Capital One's firewall would necessarily decrypt the data.

F. Defendants Claimed They Followed Reasonable Access Frequency and Retention Period

255. In Press Releases dated December 5, 2017, and October 31, 2017, Defendants stated that Capital One was ***"[a]ligned with the Consumer Financial Protection Bureau's ["CFPB"] recently released principles***" on data security ("CFPB Principles").

256. In a November 6, 2017 article published on the American Banker, Rebecca Hieronimous, Capital One's Vice President of Enterprise Digital Products and Data Connections, was quoted as saying that "***We are very aligned with the CFPB principles. As a company, we're 100% focused on ensuring that we have a secure, transparent way for our customers to access their data where they're in control.***"

257. The CFPB Principles, dated October 18, 2017, provided among other things that:

a. "Authorized terms of access, storage, use, and disposal are [] not overly broad, and consistent with the consumer's reasonable expectations in light of the product(s) or service(s) selected by the customer. Terms of data access include access frequency, data scope, and retention period."

b. "Consumer data are maintained in a manner and in formats that deter and protect against security breaches and prevent harm to consumers."

258. The foregoing statements, issued knowingly or with reckless disregard, were false and misleading. In fact: (a) Capital One's overbroad permissions, adopted to further its digital transformation, allowed any user with a Capital One username and password to decrypt the data lake; (b) by necessity, any user who breached Capital One's firewall would be assigned a Capital One username and password; (c) as a result, even if Capital One did encrypt data on its server, such encryption was no encryption at all because any successful breach of Capital One's firewall would necessarily decrypt the data; (d) Capital One's retention period and data scope did not comply with the customer's reasonable expectation of retention periods and data scope, in that customers applying for Capital One credit cards in 2005 would not imagine that Capital One still retained their social security numbers, among other data, fourteen years later; (e) Capital One's access frequency did not comply did not comply with the customer's reasonable expectation of access frequency, in that customers would not imagine that their data would be accessible to virtually anyone at Capital One to facilitate more rapid development of software and machine learning, as described more fully in ¶¶105-170, above.

IX. PLAINTIFF'S CLASS ACTION ALLEGATIONS

259. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a Class, consisting of all persons who purchased or acquired Capital One common stock during the Class Period, did not sell such shares prior to July

29, 2019, and were damaged thereby. Excluded from the Class are Defendants, all present and former officers and directors of Capital One and any subsidiary thereof, members of such excluded persons' families and their legal representatives, heirs, successors or assigns and any entity which such excluded persons controlled or in which they have or had a controlling interest.

260. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, Capital One securities were actively traded on the New York Stock Exchange ("NYSE"). While the exact number of Class members is unknown to Plaintiff at this time and can be ascertained only through appropriate discovery, Plaintiff believes that there are thousands of members in the proposed Class. Record owners and other members of the Class may be identified from records maintained by Capital One or its transfer agent and may be notified of the pendency of this action by mail or other forms of notice similar to that customarily used in securities class actions.

261. Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by Defendants' wrongful conduct in violation of federal law that is complained of herein.

262. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class and securities litigation. Plaintiff has no interests antagonistic to or in conflict with those of the Class.

263. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

a. whether the federal securities laws were violated by Defendants' acts as alleged herein;

b. whether statements made by Defendants to the investing public during the Class Period misrepresented material facts about the business, operations and management of Capital One;

c. whether the Individual Defendants caused Capital One to issue false and misleading financial statements during the Class Period;

d. whether Defendants acted knowingly or recklessly in issuing false and misleading financial statements;

e. whether the prices of Capital One securities during the Class Period were artificially inflated because of the Defendants' conduct complained of herein; and

f. whether the members of the Class have sustained damages and, if so, what is the proper measure of damages.

264. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to redress individually the wrongs done to them. There will be no difficulty in the management of this action as a class action.

265. Plaintiff may rely, in part, upon the presumption of reliance established by the fraud-on-the-market doctrine in that:

a. Defendants made public misrepresentations or failed to disclose material facts during the Class Period;

b. the omissions and misrepresentations were material;

c. Capital One securities are traded in an efficient market, in that;

i. Over 3 trillion of Capital One's shares were traded with heavy volume on the NYSE during the Class Period;

ii. Capital One was covered by more than 10 analysts;

iii. As an NYSE-traded stock, Capital One had a designated market maker which made a market in Capital One's shares, and in addition, more than 100 market makers made a market in Capital One's shares;

iv. Throughout the Class Period, Capital One met the requirements for filing a Registration Statement on Form S-3;

d. the misrepresentations and omissions alleged would tend to induce a reasonable investor to misjudge the value of Capital One's securities; and

e. Plaintiff and members of the Class purchased or acquired Capital One securities between the time the Defendants failed to disclose or misrepresented material facts and the time the true facts were disclosed, without knowledge of the omitted or misrepresented facts.

266. Based upon the foregoing, Plaintiff and the members of the Class are entitled to a presumption of reliance upon the integrity of the market.

267. Alternatively, Plaintiff and the members of the Class are entitled to the presumption of reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United States*, 406 U.S. 128, 92 S. Ct. 2430 (1972), as Defendants omitted material information.

COUNT I

For Violations of Section 10(b) And Rule 10b-5 Promulgated Thereunder Against All Defendants

268. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

269. This Count is asserted against Defendants is based upon Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC.

270. During the Class Period, Defendants, individually and in concert, directly or indirectly, disseminated or approved the false statements specified above, which they knew or deliberately disregarded were misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

271. Defendants violated §10(b) of the 1934 Act and Rule 10b-5 in that they:

a. employed devices, schemes and artifices to defraud;

b. made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or

c. engaged in acts, practices and a course of business that operated as a fraud or deceit upon plaintiff and others similarly situated in connection with their purchases of Capital One securities during the Class Period.

272. Defendants acted with scienter in that they knew that the public documents and statements issued or disseminated in the name of Capital One were materially false and misleading; knew that such statements or documents would be issued or disseminated to the investing public; and knowingly and substantially participated, or acquiesced in the issuance or dissemination of such statements or documents as primary violations of the securities laws. These defendants by virtue of their receipt of information reflecting the true facts of Capital One, their control over, and/or receipt and/or modification of Capital One's allegedly materially misleading statements,

and/or their associations with the Company which made them privy to confidential proprietary information concerning Capital One, participated in the fraudulent scheme alleged herein.

273. Individual Defendants, who are the senior officers and/or directors of the Company, had actual knowledge of the material omissions and/or the falsity of the material statements set forth above, and intended to deceive Plaintiff and the other members of the Class, or, in the alternative, acted with reckless disregard for the truth when they failed to ascertain and disclose the true facts in the statements made by them or other Capital One personnel to members of the investing public, including Plaintiff and the Class.

274. The Company is liable for the acts of the Individual Defendants and its employees, including Brady, Hieronimous, Crawford, Norris, and Blackley, under the doctrine of *respondeat superior* and common law principles of agency because all of the wrongful acts complained of herein were carried out within the scope of their employment.

275. The scienter of the Individual Defendants and other employees and agents of the Company, including Brady, Hieronimous, Crawford, Norris, and Blackley, is similarly imputed to the Company under respondeat superior and agency principles.

276. As a result of the foregoing, the market price of Capital One securities was artificially inflated during the Class Period. In ignorance of the falsity of Defendants' statements, Plaintiff and the other members of the Class relied on the statements described above and/or the integrity of the market price of Capital One securities during the Class Period in purchasing Capital One securities at prices that were artificially inflated as a result of Defendants' false and misleading statements.

277. Had Plaintiff and the other members of the Class been aware that the market price of Capital One securities had been artificially and falsely inflated by Defendants' misleading

statements and by the material adverse information which Defendants did not disclose, they would not have purchased Capital One securities at the artificially inflated prices that they did, or at all.

278. As a result of the wrongful conduct alleged herein, Plaintiff and other members of the Class have suffered damages in an amount to be established at trial.

279. By reason of the foregoing, Defendants have violated Section 10(b) of the 1934 Act and Rule 10b-5 promulgated thereunder and are liable to the plaintiff and the other members of the Class for substantial damages which they suffered in connection with their purchase of Capital One securities during the Class Period.

COUNT II

Violations of Section 20(a) of the Exchange Act Against the Individual Defendants

280. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

281. During the Class Period, the Individual Defendants participated in the operation and management of Capital One, and conducted and participated, directly and indirectly, in the conduct of Capital One's business affairs. Because of their senior positions, they knew the adverse non-public information about Capital One's misstatement of revenue and profit and false financial statements.

282. As officers and/or directors of a publicly owned company, the Individual Defendants had a duty to disseminate accurate and truthful information with respect to Capital One's financial condition and results of operations, and to correct promptly any public statements issued by Capital One which had become materially false or misleading.

283. Because of their positions of control and authority as senior officers, the Individual Defendants were able to, and did, control the contents of the various reports, press releases and public filings which Capital One disseminated in the marketplace during the Class Period

concerning Capital One's results of operations. Throughout the Class Period, the Individual Defendants exercised their power and authority to cause Capital One to engage in the wrongful acts complained of herein. The Individual Defendants therefore, were "controlling persons" of Capital One within the meaning of Section 20(a) of the Exchange Act. In this capacity, they participated in the unlawful conduct alleged which artificially inflated the market price of Capital One securities.

284. By reason of the above conduct, the Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act for the violations committed by Capital One.

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class, prays for judgment and relief as follows:

a. declaring this action to be a proper class action, designating plaintiff as Lead Plaintiff and certifying plaintiff as a class representative under Rule 23 of the Federal Rules of Civil Procedure and designating plaintiff's counsel as Lead Counsel;

b. awarding damages in favor of plaintiff and the other Class members against all defendants, jointly and severally, together with interest thereon;

c. awarding plaintiff and the Class reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

d. awarding plaintiff and other members of the Class such other and further relief as the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff hereby demands a trial by jury.

Dated: January 17, 2020

Respectfully submitted,

THE LAW FIRM OF CARLTON F. BENNETT, P.L.L.C.

/s/ Carlton F. Bennett
Carlton F. Bennett (Va. Bar No. 18453))
120 South Lynnhaven Road, Suite 100
Virginia Beach, VA 23452
Phone: (757) 266-5149
Fax: (757) 486-8910
Email: cbennett@carltonbennettlaw.com

Virginia Counsel for Plaintiff

THE ROSEN LAW FIRM, P.A.

Laurence M. Rosen (*pro hac vice* to be filed)
Phillip Kim
Jonathan Horne
275 Madison Avenue, 40th Floor
New York, New York 10016
Telephone: (212) 686-1060
Fax: (212) 202-3827
Email: lrosen@rosenlegal.com
Email: pkim@rosenlegal.com
Email: jhorne@rosenlegal.com

Lead Counsel for Plaintiff and the putative class

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing was served by the Court's CM/ECF System on counsel of record on 17th day of January 2020.

/s/ Carlton F. Bennett